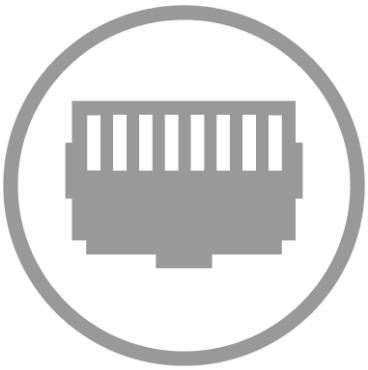
pakedge®

MS Series

LAYER 3 SWITCHES WITH OVRC

MS-1212, MS-2424, MS-2400, MS-2416, MS-4424

Command Line Interface Guide



Contents

1. Console and Telnet Administration Interface

This chapter discusses many of the features used to manage the Switch and explains many concepts and important points regarding these features. Configuring the Switch to implement these concepts is discussed in detail in later chapters.

The command-line interface (CLI) provides a text-based way to manage and monitor the switch features. You can access the CLI by using a direct connection to the console port or by using a Telnet or SSH client. To access the switch by using Telnet or Secure Shell (SSH), the switch must have an IP address configured on the network interface, and the management station you use to access the device must be able to ping the switch IP address. DHCP is enabled by default on the network VLAN.

1.1. Local Console Management

Local console management involves the administration of the Switch via a direct connection to the RS-232 DCE console port. This is an Out-of-band connection, meaning that it is on a different circuit than normal network communications, and thus works even when the network is down.

The local console management connection involves a terminal or PC running terminal emulation software to operate the Switch's built-in console program (see Chapter 5). Using the console program, a network administrator can manage, control, and monitor many functions of the Switch. Hardware components in the Switch allow it to be an active part of a manageable network. These components include a CPU, memory for data storage, other related hardware, and SNMP agent firmware. Activities on the Switch can be monitored with these components, while the Switch can be manipulated to carry out specific tasks.

1.2. Set up Your Switch Using Console Access

Out-of-band management requires connecting a terminal, such as a VT-100 or a PC running a terminal-emulation program (such as HyperTerminal, which is automatically installed with Microsoft Windows) to the RS-232 DCE console port of the Switch. Switch management using the RS-232 DCE console port is called *Local Console Management* to differentiate it from management done via management platforms, such as DView or HP OpenView.

Make sure the terminal or PC you are using to make this connection is configured to match these settings. If you are having problems making this connection on a PC, make sure the emulation is set to VT-100 or ANSI. If you still don't see anything, try pressing <Ctrl> + r to refresh the screen.

First-time configuration must be carried out through a console, that is, either (a) a VT100-type serial data terminal, or (b) a computer running communications software set to emulate a VT100. The console must be connected to the Diagnostics port. This is an RS-232 port with a 9-socket D-shell connector and DCE-type wiring. Make the connection as follows:

1. Obtain suitable cabling for the connection. You can use a null-modem RS-232 cable or an ordinary RS-232 cable and a null-modem adapter. One end of the cable (or cable/adapter combination) must have a 9-pin D-shell connector suitable for the Diagnostics port; the other end must have a connector suitable for the console's serial communications port.

2. Power down the devices, attach the cable (or cable/adapter combination) to the correct ports, and restore power.

3. Set the console to use the following communication parameters for your terminal:

    - The console port is set for the following configuration:
    - Baud rate: 115,200
    - Data width: 8 bits
    - Parity: none
    - Stop bits: 1
    - Flow Control: none

1.3. Set up Your Switch Using Telnet Access

Once you have set an IP address for your Switch, you can use a Telnet program (in a VT-100 compatible terminal mode) to access and control the Switch. The port number for Telnet is 23. Most of the screens are identical, whether accessed from the console port or from a Telnet interface.

1.3.1. Accessing the Switch CLI through the Network

Remote management of the switch is available through the network interface. To use telnet , SSH , or SNMP for switch management, the switch must be connected to the network, and you must know the IP or IPv6 address of the management interface. The switch has no IP address by default. The DHCP client on the network vlan is enabled, and the DHCP client on the network interface is disabled.

1.3.2. Using the Network Interface for Remote Management

You can manage the switch through the production network, which is known as in-band management, because in-band management traffic is mixed in with production network traffic, it is subject to all of the filtering rules usually applied on a switched/routed port such as ACLs and VLAN tagging. You can access the in-band network management interface through a connection to any front-panel port.

1.3.2.1. *Configuring the In-Band Network Interface*

To use a DHCP server to obtain the IP address, subnet mask, and default gateway information, use:

network protocol dhcp

and Use below command to display the ip address information.

Show network

2. Command Line Interface Structure and Mode-based CLI

The Command Line Interface (CLI) syntax, conventions, and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

2.1. CLI Command Format

Commands are followed by values, parameters, or both.

Example 1

ip address <ipaddr> <netmask> [<gateway>]

- **ip address** is the command name.
- **<ipaddr> <netmask>** are the required values for the command.
- **[<gateway>]** is the optional value for the command.

Example 2

snmp-server location <loc>

- **snmp-server location** is the command name.
- **<loc>** is the required parameter for the command.

Example 3

clear vlan

- **clear vlan** is the command name.

Command

The text in bold, non-italic font must be typed exactly as shown.

2.2. CLI Mode-based Topology

2.2.1. Parameters

Parameters are order dependent.

The text in bold italics should be replaced with a name or number. To use spaces as part of a name parameter, enclose it in double quotes like this: "System Name with Spaces".

Parameters may be mandatory values, optional values, choices, or a combination.

- **<parameter>.**

  The <> angle brackets indicate that a mandatory parameter must be entered in place of the brackets and text inside them.

- **[parameter].**

  The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.

- **{choice1 | choice2}.**

  The | indicates that only one of the parameters should be entered.

  The {} curly braces indicate that a parameter must be chosen from the list of choices.

2.2.2. Values

- **ipaddr**

  This parameter is a valid IP address, made up of four decimal bytes ranging from 0 to 255. The default for all IP parameters consists of zeros (that is, 0.0.0.0). The interface IP address of 0.0.0.0 is invalid.

- **macaddr**

  The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

- **areaid**

  Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network number of the sub-netted network may be used for the area ID.

- **routerid**

  The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

- **slot/port**

  This parameter denotes a valid slot number, and a valid port number. For example, 0/1 represents unit number 1, slot number 0 and port number 1. The <slot/port> field is composed of a valid slot number and a valid port number separated by a forward slash (/).

- **logical slot/port**

  This parameter denotes a logical slot number, and logical port number assigned. This is applicable in the case of a port-channel (LAG). The operator can use the logical slot number, and the logical port number to configure the port-channel.

2.2.3. Conventions

Network addresses are used to define a link to a remote host, workstation, or network. Network addresses are shown using the following syntax:

Table 4-1. Network Address Syntax

Address Type	Format	Range
IPAddr	A.B.C.D	0.0.0.0 to 255.255.255.255
MacAddr	YY:YY:YY:YY:YY:YY	hexadecimal digit pairs

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings (“”) are not valid user defined strings. Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> (command completion).

The value 'Err' designates that the requested value was not internally accessible. This should never happen and indicates that there is a case in the software that is not handled correctly.

The value of '-----' designates that the value is unknown.

2.2.4. Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (‘!’) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ‘!’ is recognized as a comment line and ignored by the parser.

Some examples are provided below:

! Script file for displaying the ip interface

! Display information about interfaces

show ip interface 0/1 !Displays the information about the first interface

! Display information about the next interface

show ip interface 0/2

! End of the script file

3. Switching Commands

3.1. System Information and Statistics Commands

This section describes the commands that use to display system information or statistics.

3.1.1. Show process cpu

This command provides the percentage utilization of the CPU by different tasks.

Format show process cpu

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show process cpu

Memory and Process CPU Utilization Info of Unit:1

Memory Utilization Report
status     KBytes
------ ----------
free      1277836
alloc      792756
CPU Utilization:

PID        Name                 5 Secs  60 Secs 300 Secs
---------- ------------------- -------- -------- --------
10         (rcu_sched)          0.00%    0.06%    0.07%
15         (kworker/1:0)        0.00%    0.01%    0.00%
52         (kworker/0:1)        0.00%    0.01%    0.02%
232        (hwmon0)             0.00%    0.01%    0.02%
613        (procmgr)            0.00%    0.08%    0.09%
720        osapiTimer           0.10%    0.11%    0.12%
729        bcmINTR              0.10%    0.07%    0.06%
730        socdmadesc.0         0.20%    0.14%    0.13%
733        bcmMEM_SCAN.0        0.00%    0.04%    0.07%
735        bcmL2X.0             3.11%    3.47%    3.49%
737        bcmCNTR.0            1.24%    1.50%    1.50%
740        bcmLINK.0            2.80%    2.65%    2.64%
741        bcmRX                0.00%    0.07%    0.07%
742        cpuUtilMonitorTask   0.20%    0.24%    0.25%
744        tL7Timer0            0.00%    0.03%    0.03%
```

```
750         simPts_task             0.00%     0.04%     0.04%
753         BootP                   0.10%     0.01%     0.00%
760         emWeb                   0.10%     0.01%     0.01%
774         hapiBroadBfdCtrlTas     0.31%     0.29%     0.29%
796         dot1s_timer_task        0.00%     0.06%     0.06%
800         radius_task             0.00%     0.02%     0.01%
806         snoopTask               0.00%     0.06%     0.07%
812         SNTP                    0.10%     0.01%     0.00%
827         pbrProcessingTask       0.00%     0.01%     0.00%
851         (ospf_app)              0.00%     0.01%     0.02%
888         RMONTask                0.00%     0.21%     0.28%
900         mlagTxTask              0.10%     0.01%     0.00%
924         openrTask               1.66%     1.86%     1.93%
--------------------------- -------- -------- --------
Total CPU Utilization          10.16%    11.30%    11.53%

(Pakedge-MS-1212-189667) #
```

3.1.2. Show process cpu threshold

This command displays the configurations of CPU utilization threshold.

Format show process cpu

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show process cpu threshold

CPU Utilization Monitoring Parameters
Rising Threshold.............................. 90 %
Rising Interval............................... 3600 secs
Falling Threshold............................. 50 %
Falling Interval.............................. 300 secs

CPU Free Memory Monitoring Threshold.......... 0 KB

(Pakedge-MS-1212-189667) #
```

3.1.3. Show eventlog

This command displays the event log, which contains error messages from the system.

Format show eventlog

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show eventlog

                                                                    Time
       File                          Line TaskID   Code     yyyy/mm/dd hh:mm:ss
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/07 21:22:57
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/07 17:38:56
EVENT> Manual Reload!                   0 48407104 00000000 2016/06/07 17:36:12
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/07 17:12:40
EVENT> Manual Reload!                   0 48407104 00000000 2016/06/07 17:09:45
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/05 00:04:36
EVENT> Manual Reload Warm!              0 48407104 00000000 2016/06/05 00:01:42
EVENT> Boot!                            0 48407104 AAAAAAAA 2016/06/04 23:38:07
EVENT> Manual Reload Warm!              0 48474A24 00000000 2016/06/04 23:35:09
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/04 22:01:35
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/02 18:09:26
EVENT> Boot!                            0 48474A24 AAAAAAAA 2016/06/02 03:26:04
EVENT> Boot!                            0 48465024 AAAAAAAA 2016/06/01 21:29:27
EVENT> Clear Event Log!                 0 48465024 AAAAAAAA 2016/05/31 23:07:58

(Pakedge-MS-1212-189667) #
```

3.1.4. Show running-config

This command is used to display/capture the current setting of different protocol packages supported on switch. This command displays/captures only commands with settings/configurations with values that differ from the default value. The output is displayed in script format, which can be used to configure another switch with the same configuration.

The paramenter “<scriptname>” means to redirect the current settings to a script file with an assigned name <scriptname>, which needs a fixed file name extension “.scr”.

The paramenter “all” means to display/capture of all commands with settings/configurations that include values that are same as the default values.

The paramenter “control-plane” means to display the running config of control-plane interface.

The paramenter “mlag” means to display the running config of Multi-Chassis Link Aggregation (MLAG).

Format show running-config [<scriptname> | all | interface {<slot/port> |lag<lag-id> | vlan <vlan-id>}]

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show running-config

!Current Configuration:
!
!System Description ", Runtime Code 18.09, Linux 3.8.13-rt9, U-Boot 2010.12 (Oct 03 2014 -
14:38:07) - ONIE 2014.05.03-7"
!System Software Version "18.09"
!System Up Time          "0 days 0 hrs 9 mins 53 secs"
!Cut-through mode is configured as disabled
!Additional Packages     BGP-4,QOS,Multicast,IPv6,Routing,Data Center
!Current SNTP Synchronized Time: SNTP Client Mode Is Disabled
!
configure
interface vlan 1
exit
vlan database
exit

sntp clock timezone "Taipei" 8 0 before-utc
time-range
line console
exit

line vty
exit

line ssh
exit

interface vlan 1
exit
!
interface control-plane
exit
router ospf
exit
ipv6 router ospf
exit
exit

(Pakedge-MS-1212-189667) #
```

3.1.5. Show sysinfo

This command displays switch brief information and MIBs supported.

Format show sysinfo

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show sysinfo

System Description.............................. MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE), 0.01.0.100045, Linux 3.6.5
System Name..................................... Pakedge-MS-1212-189667
System Location.................................
System Contact..................................
System Object ID................................ 1.3.6.1.4.1.39221.1.1
System Up Time.................................. 0 days 3 hrs 7 mins 45 secs
Current SNTP Synchronized Time.................. Dec  9 10:42:59 2019 UTC

MIBs Supported:

RFC 1907 - SNMPv2-MIB               The MIB module for SNMPv2 entities
HC-RMON-MIB                         The original version of this MIB, published
                                    as RFC3273.
HCNUM-TC                            A MIB module containing textual conventions
                                    for high capacity data types.
SNMP-COMMUNITY-MIB                  This MIB module defines objects to help
                                    support coexistence between SNMPv1, SNMPv2,
                                    and SNMPv3.
SNMP-MPD-MIB                        The MIB for Message Processing and
                                    Dispatching
SNMP-TARGET-MIB                     The Target MIB Module
SNMP-VIEW-BASED-ACM-MIB             The management information definitions for
                                    the View-based Access Control Model for SNMP.
PAKEDGE-POWER-ETHERNET-MIB          PAKEDGE Power Ethernet Extensions MIB
PAKEDGE-BOXSERVICES-PRIVATE-MIB     The PAKEDGE Private MIB for PAKEDGE Box
                                    Services Feature.
IANA-ADDRESS-FAMILY-NUMBERS-MIB     The MIB module defines the
                                    AddressFamilyNumbers textual convention.
PAKEDGE-DENIALOFSERVICE-PRIVATE-M   The PAKEDGE Private MIB for PAKEDGE Denial
IB                                  of Service.
LLDP-MIB                            Management Information Base module for LLDP
                                    configuration, statistics, local system data
                                    and remote systems data components.
LLDP-EXT-MED-MIB                    The LLDP Management Information Base
                                    extension module for TIA-TR41.4 Media
                                    Endpoint Discovery information.
DNS-SERVER-MIB                      The MIB module for entities implementing the
                                    server side of the Domain Name System (DNS)
                                    protocol.
SMON-MIB                            The MIB module for managing remote
```

```
                                monitoring device implementations for
                                Switched Networks
PAKEDGE-TIMERANGE-MIB           The PAKEDGE Private MIB for PAKEDGE Time
                                Ranges
DISMAN-TRACEROUTE-MIB           The Traceroute MIB (DISMAN-TRACEROUTE-MIB)
                                provides access to the traceroute capability
                                at a remote host.
LAG-MIB                         The Link Aggregation module for managing
                                IEEE 802.3ad
RFC 1493 - BRIDGE-MIB           Definitions of Managed Objects for Bridges
                                (dot1d)
RFC 2674 - Q-BRIDGE-MIB         The VLAN Bridge MIB module for managing
                                Virtual Bridged Local Area Networks
RFC 2863 - IF-MIB               The Interfaces Group MIB using SMIv2
PAKEDGE-SWITCHING-MIB           PAKEDGE Switching - Layer 2
PAKEDGE-PORTSECURITY-PRIVATE-MIB Port Security MIB.
IANAifType-MIB                  This MIB module defines the IANAifType
                                Textual Convention
MAU-MIB                         Management information for 802.3 MAUs.
PAKEDGE-SNTP-CLIENT-MIB         Defines PAKEDGE Corporation enterprise OID
                                pertaining to SNTP client configuration and
                                statistical collection.
PAKEDGE-DOT1X-ADVANCED-FEATURES-M The PAKEDGE Private MIB for PAKEDGE Dot1x
IB                              Advanced Features
PAKEDGE-RADIUS-AUTH-CLIENT-MIB  The PAKEDGE Private MIB for PAKEDGE Radius
                                Authentication Client.
RADIUS-AUTH-CLIENT-MIB          RADIUS Authentication Client MIB
PAKEDGE-MANAGEMENT-ACAL-MIB     The PAKEDGE Private MIB for PAKEDGE
                                management acal feature.
PAKEDGE-ROUTING-MIB             PAKEDGE Routing - Layer 3
IP-FORWARD-MIB                  The MIB module for the management of CIDR
                                multipath IP Routes.
PAKEDGE-QOS-MIB                 PAKEDGE Flex QOS Support
PAKEDGE-QOS-COS-MIB             PAKEDGE Flex QOS COS
PAKEDGE-QOS-DIFFSERV-PRIVATE-MIB PAKEDGE Flex QOS DiffServ Private MIBs'
                                definitions
draft-ietf-magma-mgmd-mib-03    MGMD MIB, includes IGMPv3 and MLDv2.
RFC 5240 - PIM-BSR-MIB          Bootstrap Router mechanism for PIM routers
IANA-RTPROTO-MIB                IANA IP Route Protocol and IP MRoute
                                Protocol Textual Conventions
IPMROUTE-STD-MIB                The MIB module for management of IP
                                Multicast routing, but independent of the
                                specific multicast routing protocol in use.
(Pakedge-MS-1212-189667) #
```

3.1.6. Show tech-support

Use this command displays switch system information and configurations when you contact technical support. The output of the show tech-support command combines the output of the following commands:

show version, show sysinfo, show interface status, show logging, show event log, show logging buffered, show trap log, show running config, … etc

The parameter “file” means to write the output into a file with file name “TechSupport”.

Other parameters are used to display the information of assigned component.

Format show tech-support [{dot1q | dot1s | dot3ad | layer3 | link_dependency | lldp | log | qos |routing | sim | switching | system} [file] | file]

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) # show tech-support

*************** show version ***************

Switch: 1

System Description.............................. MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE), 0.01.0.100045, Linux 3.6.5
Machine Type.................................... MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE)
Machine Model................................... MS-1212
Serial Number................................... E8C74F189667881943203002789BL
Maintenance Level............................... A
Manufacturer.................................... 0xbc00
Burned In MAC Address........................... E8:C7:4F:18:96:67
Software Version................................ 0.01.0.100045
Operating System................................ Linux 3.6.5
Network Processing Device....................... BCM53346_A0
Additional Packages............................. LITENOS QOS
                                                 LITENOS Multicast
                                                 LITENOS IPv6 Management
                                                 LITENOS Routing
                                                 LITENOS OpEN API
*************** show sysinfo ***************


System Description.............................. , Runtime Code 0.01.0.100041
System Name.....................................
System Location.................................
System Contact..................................
System Object ID................................ 1.3.6.1.4.1.39221.1.1
System Up Time.................................. 0 days 2 hrs 2 mins 0 secs
Current SNTP Synchronized Time.................. SNTP Client Mode Is Disabled
```

```
(* note: this command displays information more than 3000 lines, so here we omit remained
   messages.)
   :
   :
(Pakedge-MS-1212-189667) #
```

3.1.7. Show hardware

This command displays inventory and hardware information for the switch.

Format show hardware

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show hardware
Switch: 1

System Description.............................. MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE), 0.01.0.100045, Linux 3.6.5
Machine Type.................................... MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE)
Machine Model................................... MS-1212
Serial Number................................... E8C74F189667881943203002789BL
Maintenance Level............................... A
Manufacturer.................................... 0xbc00
Burned In MAC Address........................... E8:C7:4F:18:96:67
Software Version................................ 0.01.0.100045
Operating System................................ Linux 3.6.5
Network Processing Device....................... BCM53346_A0
Additional Packages............................. LITENOS QOS
                                                 LITENOS Multicast
                                                 LITENOS IPv6 Management
                                                 LITENOS Routing
                                                 LITENOS OpEN API
(Pakedge-MS-1212-189667) #
```

3.1.8. Show version

This command displays inventory, software packages and license key information for the switch.

Format show version

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show version

Switch: 1

System Description..............................  MS-1212 Gigabit Ethernet POE Switch(12 GE + 2
XE), 0.01.0.100045, Linux 3.6.5
Machine Model...................................  MS-1212
Serial Number...................................  E8C74F189667881943203002789BL
Manufacturer....................................  GCOM
Burned In MAC Address...........................  E8:C7:4F:18:96:67
Software Version................................  0.01.0.100045
Operating System................................  Linux 3.6.5
Bakpak Cloud ID.................................  MS-1212C0919A11367(Pakedge-MS-1212-189667) #
```

3.1.9. Show loginsession

This command displays serial port or remote login connections to the switch.

The parameter “long” means to display full user names of login sessions.

Format show loginsession [long]

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show loginsession

ID   User Name     Connection From       Idle Time  Session Time Session Type
---- ------------ --------------------- ---------- ------------ ------------
00   admin         EIA-232               00:00:00   02:08:12     Serial
01   guest         172.16.3.68           00:00:05   00:00:05     SSH

(Pakedge-MS-1212-189667) #
```

3.1.10. Show command filter

All commands starting with keyword “show” can use below parameters to refine output or redirect output to a file. Following any show command to use symbol “|” to set filter and it uses regular expression to math assigned keyword.

The parameter “commands” means any show command of CLI.

The parameter "**|**" means to use filter option.

The parameter "begin" sets output to begin with the line that matches assigned keyword.

The parameter "exclude" sets output to exclude lines that matches assigned keyword.

The parameter "include" sets output to include lines that matches assigned keyword only.

The parameter "section" sets output to only include a specified section of the content (e.g., "interface 0/1") with a configurable end-of-section delimiter.

Format show command **|** {[begin <keyword>] [exclude <keyword>] [include <keyword>][section <starting keyword> [ending keyword]] }

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show interface ethernet 0/1 | begin "Total Packets" exclude "0"

Total Packets Received (Octets)..... 438677
Packets Received 64 Octets..... 115
Packets Received 65-127 Octets..... 376
Packets Received 128-255 Octets..... 2136
Packets RX and TX 64 Octets..... 117
Packets RX and TX 65-127 Octets..... 36293
Packets RX and TX 128-255 Octets..... 2136

Total Packets Received Without Errors..... 2729
Multicast Packets Received..... 2258
Broadcast Packets Received..... 471

Packets Discarded by Chip Debug Counter..... 225

Total Received Packets Discarded..... 225

Packets Transmitted 64 Octets..... 2
Packets Transmitted 65-127 Octets..... 35917
Max Frame Size..... 1518

Total Packets Transmitted Successfully..... 35919
Multicast Packets Transmitted..... 35919

MSTP BPDUs Transmitted..... 33675

(Pakedge-MS-1212-189667) #
```

3.2. Device Configuration Commands

3.2.1. Network VLAN commands

3.2.1.1. *network parms*

This command sets the IP address, subnet mask and gateway of the device. The IP address and the gateway must be on the same subnet. When you specify the `none` option, the IP address and subnet mask are set to the factory defaults.

Format `network parms {ipaddr netmask [gateway]| none}`
Mode Privileged EXEC

3.2.1.2. *network protocol*

This command specifies the network configuration protocol to be used. If you modify this value, change is effective immediately. If you use the *bootp* parameter, the switch periodically sends requests to a BootP server until a response is received. If you use the *dhcp* parameter, the switch periodically sends requests to a DHCP server until a response is received. If you use the *none* parameter, you must configure the network information for the switch manually.

Default none

Format `network protocol {none | bootp | dhcp}`
Mode Privileged EXEC

3.2.1.3. *network protocol dhcp*

This command enables the DHCPv4 client on a Network port. If the `client-id` optional parameter is given, the DHCP client messages are sent with the client identifier option.

Default none

Format `network protocol dhcp [client-id]` **Mode** Global Config

There is no support for the **no** form of the command **network protocol dhcp client-id**. To remove the `client- id` option from the DHCP client messages, issue the command **network protocol dhcp** without the `client-id` option. The command **network protocol none** can be used to disable the DHCP client and client-id option on the interface.

Example: The following shows an example of the command.

```
(Routing) # network protocol dhcp client-id
```

3.2.1.4. *network mac-address*

This command sets locally administered MAC addresses. The following rules apply:

- Bit 6 of byte 0 (called the U/L bit) indicates whether the address is universally administered (b'0') or locally

  administered (b'1').

- Bit 7 of byte 0 (called the I/G bit) indicates whether the destination address is an individual address (b'0') or

  a group address (b'1').

- The second character, of the twelve character macaddr, must be 2, 6, A or E.

A locally administered address must have bit 6 On (b'1') and bit 7 Off (b'0').

Format `network mac-address` *macaddr*

Mode Privileged EXEC

3.2.1.5. *network mac-type*

This command specifies whether the switch uses the burned in MAC address or the locally-administered MAC address.

Default burnedin

Format `network mac-type {local | burnedin}`

Mode Privileged EXEC

no network mac-type

This command resets the value of MAC address to its default.

Format `no network mac-type`

Mode Privileged EXEC

3.2.1.6. *show network*

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed. The network interface is always considered to be up, whether

or not any member ports are up; therefore, the show network command will always show **Interface Status** as **Up**.

Format `show network`

Modes
- Privileged EXEC
- User EXEC

```
(admin) #show network


Interface Status.............................. Up

IP Address.................................... 10.250.3.1

Subnet Mask................................... 255.255.255.0

Default Gateway............................... 10.250.3.3

IPv6 Administrative Mode...................... Enabled

IPv6 Prefix is ..............................
fe80::210:18ff:fe82:64c/64
IPv6 Prefix is ............................... 2003::1/128

IPv6 Default Router is .......................
fe80::204:76ff:fe73:423a
Burned In MAC Address.........................
00:10:18:82:06:4C

Locally Administered MAC address..............
00:00:00:00:00:00

MAC Address Type.............................. Burned In

Configured IPv4 Protocol ..................... None

Configured IPv6 Protocol ..................... DHCP

DHCPv6 Client DUID ...........................
00:03:00:06:00:10:18:82:06:4C IPv6 Autoconfig
Mode.......................... Disabled

Management VLAN ID............................ 1

DHCP Client Identifier........................ 0fastpath-
0010.1882.160B-vl1
```

3.2.2. Interface show commands

3.2.2.1. *Show interfaces status*

The command displays a summary of information for a specific interface or all interfaces.

Format show interfaces status [{<slot/port> |all |lag <lag-id> | vlan <vlan-id>}]

Parameter	Definition
<slot/port>	Specifies Interface number .
all	To display information for all interfaces.
lag <1-6>	Specifies to display information for the lag interfaces. The range of the lag ID is 1 to 6.
vlan <vlan-id>	Specifies to display information for the vlan interfaces. The range of the VLAN ID is 1 to 4093.

Mode Privileged EXEC

The following will show the information of each command with a different parameter.

3.2.2.1.1. Show interfaces status all

Displays information for all interfaces.

Fields	Definition
Intf	The physical slot and physical port.
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: **Source:** This port is a monitoring port. **PC Mbr:** This port is a member of a port-channel (LAG). **Dest:** This port is a probe port.
Admi Mode (Admin Mode)	Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. It may be enabled or disabled. The factory default is enabled.

Phy Mode (Physical Mode)	Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex 100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
Phy Stat	Indicates the port speed and duplex mode.
Link Stat	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Mode	Displays flow control mode.
Cap. Status (Capabilities Status)	Displays interface capabilities the port supports.

3.2.2.1.2. Show interface status <slot/port>

Displays information for a specific interface.

Fields	Definition
Interface	The physical slot and physical port.
ifIndex	Displays the interface index associated with the port.
Description	Description string attached to a port. It can be of up to 64 characters in length.
Admin Mode	Selects the Port control administration state. The port must be enabled in order for it to be allowed into the network. It may be enabled or disabled. The factory default is enabled.
Physical Mode	Selects the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex 100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.
Physical Status	Indicates the port speed and duplex mode.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.

Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays interface mac address.
Bit Offset Val	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.
MDI Status	Displays interface MDI status.
MDI Config	Displays interface MDI mode.

3.2.2.1.3. Show interface status lag <1-6>

Displays information for the lag interface.

Fields	Definition
Interface	The interface name.
ifIndex	Displays the interface index associated with the port.
Description	Description string attached to the port-channel. It can be of up to 64 characters in length.
Admin Mode	Displays the lag control administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	Indicates whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.

Capability Information	Displays interface capabilities.
Bit Offset Val	Displays the bit offset value which corresponds to the port when the MIB object type PortList is used to manage in SNMP.

3.2.2.1.4. Show interface status vlan <1-4093>

Displays information for the vlan interface.

Fields	Definition
Interface	The interface name.
ifIndex	Displays the interface index associated with the interface.
Description	Description string attached to an interface .
Admin Mode	Displays the administration state.
Physical Mode	The speed and duplex mode setting on the interface.
Physical Status	Indicates the speed and duplex mode for the physical interface.
Cable Type	Displays interface cable type.
Link Status	Indicates whether the Link is up or down.
Link Trap	This object determines whether to send a trap when link status changes. The factory default is enabled.
LACP Mode	Displays whether LACP is enabled or disabled on this port.
Flow Control Mode	Displays flow control mode.
Capability Information	Displays interface capabilities.
MAC Address	Displays interface mac address.
Bit Offset Val	Displays the bit offset value which corresponds to the interface when the MIB object type PortList is used to manage in SNMP.

3.2.2.2. *Show interface counters*

This command reports key summary statistics for all the ports (physical/CPU/port-channel).

Format `show interface counters`

Term	*Description*
Port	The interface associated with the rest of the data in the row.
InOctects	The total number of octets received on the interface.
InUcastPkts	The total number of unicast packets received on the interface.
InMcastPkts	The total number of multicast packets received on the interface.
InBcastPkts	The total number of broadcast packets received on the interface.
OutOctects	The total number of octets transmitted by the interface.
OutUcastPkts	The total number of unicast packets transmitted by the interface.
OutMcastPkts	The total number of multicast packets transmitted by the interface.
OutBcastPkts	The total number of broadcast packets transmitted by the interface.

Mode Privileged EXEC

3.2.2.3. *Show interface dampening*

This command displays the status and configured parameters of the interfaces configured with dampening.

The CLI command “clear counters” resets the flap counter to zero.

The interface CLI command “no shutdown” reset the suppressed state to False.

Any change in the dampening configuration resets the current penalty, reuse time and suppressed state to their default value, meaning 0, 0, and False respectively.

Format show interface dampening

Mode Privileged EXEC

Display Message

Fields	Definition
Interface	The interface name.

Flaps	The number times the link state of an interface changed from UP to DOWN.
Penalty	Accumulated Penalty.
Supp	Indicates if the interface is suppressed or not.
ReuseTm	Number of seconds until the interface is allowed to come up again.
HalfL	Configured half-life period.
ReuseV	Configured reuse-threshold.
SuppV	Configured suppress threshold.
MaxSTm	Configured maximum suppress time in second.
MaxP	Maximum possible penalty.
Restart	Configured restart penalty .

3.2.2.4. *Show interface lag*

Use this command to display configuration information about the specified LAG interface.

Format `show interface lag` *lag-intf-num*

Mode Privileged EXEC

Display Message

Parameters	*Definition*
Packets Received Without Error	The total number of packets (including broadcast packets and multicast packets) received on the LAG interface
Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.
Receive Packets Discarded	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Packets Transmitted Without Error	The total number of packets transmitted out of the LAG
Transmit Packets Discarded	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higherlayer protocol. A possible reason for discarding a packet could be to free up buffer space.
Transmit Packets Errors	The number of outbound packets that could not be transmitted because of errors.
Collisions Frames	The best estimate of the total number of collisions on this Ethernet segment.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this LAG were last cleared.

3.2.2.5. *Show interface switchport*

This command displays a summary of statistics for all CPU traffic.

Format show interfaces switch

Mode Privileged EXEC

Parameter	Definition
Packets Received Without Error	The total number of packets received from the interface.
Broadcast Packets Received	The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.
Packets Transmitted Without Errors	The total number of packets transmitted out of the interface.
Broadcast Packets Transmitted	The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.
Transmit Packet Errors	The number of outbound packets that could not be transmitted because of errors.
Address Entries Currently in Use	The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.
VLAN Entries Currently in Use	The number of VLAN entries presently occupying the VLAN table.
Time Since Counters Last Cleared	The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

3.2.2.6. *Show port*

This command displays port information.

Format show port {intf-range | all}

Mode Privileged EXEC

Display Message

Parameter Definition	Parameter Definition
Interface slot/port	Interface slot/port
Type	If not blank, this field indicates that this port is a special type of port. The possible values are: • Mirror — this port is a monitoring port. • PC Mbr— this port is a member of a port-channel (LAG). • Probe — this port is a probe port.
Admin Mode	The Port control administration state. The port must be enabled in order for it to be allowed into the network. May be enabled or disabled. The factory default is enabled.
Physical Mode	The desired port speed and duplex mode. If negotiation support is selected, then the duplex mode and speed is set from the negotiation process. Note that the maximum capability of the port (full duplex -100M) is advertised. Otherwise, this object determines the port's duplex mode and transmission rate.

Physical Status	The port speed and duplex mode.
Link Status	The Link is up or down.
Link Trap	This object determines whether or not to send a trap when link status changes. The factory default is enabled.
LACP Mode	LACP is enabled or disabled on this port.

Example: The following command shows an example of the command output for all ports.

(Pakedge-MS-1212-189667) #show port all

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Mode	Actor Timeout
0/1		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/2		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/3		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/4		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/5		Enable	10G Full		Down	Enable	Enable	long
0/6		Enable	10G Full		Down	Enable	Enable	long
0/7		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/8		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/9		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/10		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/11		Enable	10G Full		Down	Enable	Enable	long
0/12		Enable	10G Full		Down	Enable	Enable	long
0/13		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/14		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/15		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/16		Enable	10G Full	10G Full	Up	Enable	Enable	long

⋮

Example: The following command shows an example of the command output for a range of ports.

(Pakedge-MS-1212-189667) #show port 0/1-0/6

Intf	Type	Admin Mode	Physical Mode	Physical Status	Link Status	Link Trap	LACP Actor Mode	Actor Timeout
0/1		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/2		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/3		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/4		Enable	10G Full	10G Full	Up	Enable	Enable	long
0/5		Enable	10G Full		Down	Enable	Enable	long
0/6		Enable	10G Full		Down	Enable	Enable	long

3.2.2.7. *Show port advertise*

Use this command to display the local administrative link advertisement configuration, local operational link advertisement, and the link partner advertisement for an interface. It also displays priority Resolution for speed and duplex as per 802.3 Annex 28B.3. It displays the Auto negotiation state, PHY Master/Slave Clock configuration, and Link state of the port.

If the link is down, the Clock is displayed as *No Link*, and a dash is displayed against the Oper Peer advertisement, and Priority Resolution. If Auto negotiation is disabled, then the admin Local Link advertisement, operational local link advertisement, operational peer advertisement, and Priority resolution fields are not displayed.

If this command is executed without the optional *unit/slot/port* parameter, then it displays the Auto- negotiation state and operational Local link advertisement for all the ports. Operational link advertisement will display speed only if it is supported by both local as well as link partner. If auto-negotiation is disabled, then operational local link advertisement is not displayed.

Format `show port advertise [unit/slot/port]`

Mode Privileged EXEC

Example: The following commands show the command output with and without the optional parameter: `(LITEON LITENOS Switching)#show port advertise 0/1`

```
Port: 0/1

Type: Gigabit - Level
```

```
        Link State: Down

        Auto Negotiation: Enabled

        Clock: Auto

                                      1000f 1000h 100f 100h 10f 10h
        ----- ----- ---- ---- --- ---  Admin Local Link Advertisement
        no    no    yes  no   yes no  Oper Local Link Advertisement
        no    no    yes  no   yes no  Oper Peer Advertisement

        no    no    yes  yes  yes yes  Priority Resolution

        -     -     yes  -    -   -

        (LITEON LITENOS Switching)#show port advertise

        Port      Type                                  Neg      Operational Link
        Advertisement --------- ------------------------------ ----------- ------
        ------------------------

        0/1   Gigabit - Level                    Enabled  1000f, 100f, 100h,
        10f, 10h

        0/2   Gigabit - Level                    Enabled  1000f, 100f, 100h,
        10f, 10h

0/3   Gigabit - Level                    Enabled  1000f, 100f, 100h, 10f, 10h
```

3.2.2.8. *Show port description*

This command displays the interface description.

Format show port description {slot/port | port-channel <portchannel-id>}

Mode Privileged EXEC

Display Message

Parameter	Definition
Interface	The slot/port or LAG with the information to view.
ifIndex	The interface index number associated with the port.
Description	The alpha-numeric description of the interface created by the command “description” on page 30.
MAC address	The MAC address of the port. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.
Bit Offset Val	The bit offset value.

Example: The following example shows the CLI display output for the command *show port description 0/1*.

(Pakedge-MS-1212-189667) #show port description 0/1

Interface..... 0/1

ifIndex..... 1
Description……..
MAC address..... C4:54:44:45:46:AB
Bit Offset Val….. 1

3.2.2.9. *Interface configuration commands*

3.2.2.9.1. Interface

This command is used to enter Interface configuration mode.

Format interface {<slot/port> | lag <1-6> | range <intf-range>| vlan <1-4093> }

Parameter	Definition
<slot/port>	Enter into interface mode
lag <1-6>	Enter into interface lag mode.
Range <intf-range>	Enter into interface range mode.Specifies the interface(s) in slot/port format, use comma for a list and hyphen for ranges.
vlan <1-4093>	Enter into interface VLAN mode.

Mode Global Config

3.2.2.9.2. Description

This command is used to create an alpha-numeric description of the port.

Format description <description>

Parameter	Definition
<description>	an alpha-numeric description

Default None

Mode Interface Config

no description

This command removes the description of the interface.

Format no description

Mode Interface Config

3.2.2.9.3. Flowcontrol

This command enables 802.3x flow control

Format flowcontrol

Default Disabled

Mode Global Config

no flowcontrol

This command removes the flow control feature

Format no flowcontrol

Mode Global Config

3.2.2.9.4. Mtu

Use the mtu command to set the maximum transmission unit (MTU) size, in bytes, for frames that ingress or egress the interface. You can use the mtu command to configure jumbo frame support for physical and port- channel (LAG) interfaces. For the standard ICOS implementation, the MTU size is a valid integer between 1522–9198 for tagged packets and a valid integer between 1518 and 9198 for untagged packets.

Format mtu 1518-9198

Default 1518

Mode Interface Config

no mtu

This command sets the default MTU size (in bytes) for the interface.

Format no mtu

Mode Interface Config

3.2.2.9.5. Auto-Negotiate

This command enables automatic negotiation on a port.

Format auto-negotiate

Default Enable

Mode Interface Config

no auto-negotiate

This command disables automatic negotiation on a port.

Format no auto-negotiate

Mode Interface Config

Auto-negotiate all

This command enables automatic negotiation on all ports.

Format auto-negotiate all

Mode Global Config

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format no auto-negotiate all

Mode Global Config

3.2.2.9.6. Shutdown

This command is used to disable a port.

The no command is used to enables a port.

Format [no] shutdown

Parameter	Definition
no.	Reset to default.

Default Enable

Mode Interface Config

3.2.2.9.7. Shutdown all

This command is used to disable all ports.

Format [no] shutdown all

Parameter	Definition
no.	Reset to default.

Mode Global Config

3.2.2.9.8. Speed

Use this command to enable or disable auto-negotiation and set the speed that will be advertised by that port. The duplex parameter allows you to set the advertised speed for both half as well as full duplex mode.

Use the `auto` keyword to enable auto-negotiation on the port. Use the command without the `auto` keyword to ensure auto-negotiation is disabled and to set the port speed and mode according to the command values. If auto-negotiation is disabled, the speed and duplex mode must be set.

Default Auto-negotiation is enabled.

Format `speed auto {10|100|1000|10G} [half-duplex|full-duplex]`

`speed {10|100|10G} {half-duplex|full-duplex}.`

Parameter	Definition
auto	Enable auto-negotiation on the port
10	10BASE-T
100	100BASE-T
1000	1000BASE-T
full-duplex	Full duplex
half-duplex	Half duplex

Default speed auto

Mode Interface Config

speed all

This command is used to set speed and duplex on all ports. Need to use the command *no negotiate all* before issuing this command.

Format speed-duplex all {10 | 100} { full-duplex | half-duplex }

Mode Global Config

3.2.3. L2 MAC Address and Multicast Forwarding Database Tables

3.2.3.1. *Show mac-addr-table*

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. The administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

Format show mac-addr-table [{<macaddr> <vlan-id>}]

Default None

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table*.

(Pakedge-MS-1212-189667) #show mac-addr-table

VLAN ID	MAC Address	Interface	IfIndex	Status
1	C4:54:44:56:D3:57	vlan 1	136	Management

3.2.3.2. *Show mac-addr-table count*

This command displays the total forwarding database entries, the number of static and learnning mac address, and the max address available on the switch.

Format show mac-addr-table count

Default None

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table count*.

(Pakedge-MS-1212-189667) #show mac-addr-table count

Dynamic Address count..... 0

Static Address (User-defined) count..... 1

Total MAC Addresses in use..... 1

Total MAC Addresses available..... 98304

3.2.3.3. *Show mac-addr-table interface*

This command displays the forwarding database entries. The user can search FDB table by using specific interface number.

Format show mac-addr-table interface {<slot/port> | port-channel <portchannel-id> | vlan <vlan-id>}

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table vlan 1.*

(Pakedge-MS-1212-189667) #show mac-addr-table interface vlan 1

MAC Address	Interface	Status
C4:54:44:56:D3:57	vlan 1	Management

3.2.3.4. *Show mac-address-table igmpsnooping*

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format show mac-address-table igmpsnooping

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-address-table igmpsnooping.*

(Pakedge-MS-1212-189667) (Config)#show mac-address-table igmpsnooping

VLAN ID	MAC Address	Type	Description	Interfaces
00:01:01:00:5E:01:01:01	Static	Network Assist	Fwd: 0/1,ch1	
00:02:01:00:5E:AA:BB:CC	Static	Network Assist	Fwd: 0/2	

3.2.3.5. *Show mac-address-table multicast*

This command displays the MFDB information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the all parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format show mac-address-table multicast [{<macaddr> <vlan-id>]]

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-address-table multicast.*

(Pakedge-MS-1212-189667) (Config)#show mac-address-table multicast

VLAN ID	MAC Address	Source	Type	Description	Interface	Fwd Interface
1	01:00:5E:01:01:01	IGMP	Static	Network Assist	Fwd: 0/1, ch1	Fwd: 0/1, ch1
2	01:00:5E:AA:BB:CC	IGMP	Static	Network Assist	Fwd: 0/2	Fwd: 0/2

3.2.3.6. *Show mac-address-table stats*

This command displays the MFDB statistics.

Format show mac-address-table stats

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-address-table stats.*

(Pakedge-MS-1212-189667) #show mac-address-table stats

Max MFDB Table Entries..... 1024

Most MFDB Entries Since Last Reset..... 0

Current Entries..... 0

3.2.3.7. *Show forwardingdb agetime*

This command displays the forwarding database address aging timeout.

Format show forwardingdb agetime

Mode Privileged EXEC

Example: The following example shows the CLI display output for the command *show mac-addr-table agetime.*

(Pakedge-MS-1212-189667) # show forwardingdb agetime

Address Aging Timeout:300

3.2.3.8. *bridge aging-time*

This command configures the forwarding database address aging timeout in seconds.

Format bridge aging-time <10-1000000>

Default 300s

Mode Global Config

no bridge aging-time

Use this command to return the address aging timeout the default settings.

Format no bridge aging-time

Mode Global Config

3.2.4. VLAN Commands

This section describes the commands you use to configure VLAN settings.

3.2.4.1. *Vlan database*

This command gives you access to the VLAN Config mode, which allows you to configure VLAN characteristics.

Format vlan database

Mode Global Config

3.2.4.2. *Vlan*

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4093.

Format vlan <vlan-list>

Mode VLAN Config

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). The VLAN range is 1-4093.

Format no vlan <vlan-list>

Mode VLAN Config

3.2.4.3. *Vlan makestatic*

This command changes a dynamically created VLAN to a static VLAN (one that is permanently configured and defined). The ID is a valid VLAN identification number. VLAN range is 2-4093.

Format vlan makestatic <2-4093>

Mode VLAN Config

3.2.4.4. *Vlan name*

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4093.

Format vlan name <1-4093> <newname>

Default VLAN ID 1 - default
Other VLANS - blank string

Mode VLAN Config

no vlan name

This command sets the name of a VLAN to a blank string.

Format no vlan name <1-4093>

Mode VLAN Config

3.2.4.5. *Show vlan*

This command displays brief information on a list of all configured VLANs.

Format show vlan

Mode Privileged EXEC
User EXEC

Display Message

Term	Definition
VLAN ID	There is a VLAN Identifier (vlanid) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 16 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.
VLAN Type	Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface(s)	Indicates by slot id and port number which port belongs to this VLAN.

3.2.4.6. *Show vlan id*

This command displays detailed information, including interface information, for a specific VLAN.

Format show vlan {id <1-4093> | name <vlanname>}

Mode Privileged EXEC
User EXEC

Display Message

Term	Definition
VLAN ID	There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4093.
VLAN Name	A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters, including blanks. The default is blank. VLAN ID 1 is always named `Default`. This field is optional.
VLAN Type	Type of VLAN, which can be Default, (VLAN ID = 1), can be static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).
Interface	Indicates by slot id and port number which port is controlled by the fields on this line.
Current: • **Include** • **Exclude** • **Autodetect**	Determines the degree of participation of this port in this VLAN. The permissible values are: • This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Configured: • **Include** • **Exclude** • **Autodetect**	Determines the configured degree of participation of this port in this VLAN. The permissible values are: • This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard. • This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard. • Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.
Tagging: • **Tagged** • **Untagged**	Select the tagging behavior for this port in this VLAN: • Specifies to transmit traffic for this VLAN as tagged frames. • Specifies to transmit traffic for this VLAN as untagged frames.

3.2.4.7. *Show vlan internal usage*

This command displays information about the VLAN ID allocation on the switch.

Format show vlan internal usage

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
Base VLAN ID	Identifies the base VLAN ID for Internal allocation of VLANs to the routing interface.
Allocation policy	Identifies whether the system allocates VLAN IDs in ascending or descending order.

3.2.4.8. *Show interface switchport*

This command displays VLAN port information.

Format show interface switchport {<slot/port> | port-channel <1-64>}

Mode Privileged EXEC
User EXEC

Display Message

Term	Definition
Interface	Indicates by slot id and port number which port is controlled by the fields on this line. It is possible to set the parameters for all ports by using the selectors on the top line.
Native VLAN	The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is 1.
Mode	Indicates this interface is operating on Access mode or General mode.
Ingress Filtering	May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

Term	Definition
Acceptable Frame Type	Specifies the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to

	'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

3.2.5. Private VLAN Commands

This section describes the commands you use for private VLANs. Private VLANs provides Layer 2 isolation between ports that share the same broadcast domain. In other words, it allows a VLAN broadcast domain to be partitioned into smaller point-to-multipoint subdomains. The ports participating in a private VLAN can be located anywhere in the Layer 2 network.

3.2.5.1. *Switchport private-vlan*

This command defines a private-VLAN association for an isolated or community port or a mapping for a promiscuous port.

Format switchport private-vlan {host-association <primary-vlan-id> <secondary-vlan-id> | mapping <primary-vlan-id> [add | remove] <secondary-vlan-list>}

Parameter	Definition
host-association	Defines the VLAN association for community or host ports.
mapping	Defines the private VLAN mapping for promiscuous ports.
primary-vlan-id	Primary VLAN ID of a private VLAN.
secondary-vlanid	Secondary (isolated or community) VLAN ID of a private VLAN.
add	Associates the secondary VLAN with the primary one.
remove	Deletes the secondary VLANs from the primary VLAN association.
secondary-vlanlist	A list of secondary VLANs to be mapped to a primary VLAN.

Mode Interface Config

no switchport private-vlan

This command removes the private-VLAN association or mapping from the port.

Format no switchport private-vlan {host-association|mapping}

Mode Interface Config

3.2.5.2. *Switchport mode private-vlan*

This command configures a port as a promiscuous or host private VLAN port. Note that the properties of each mode can be configured even when the switch is not in that mode. However, they will only be applicable once the switch is in that particular mode.

Format switchport mode private-vlan {host|promiscuous}

Parameter	Definition
host	Configures an interface as a private VLAN host port. It can be either isolated or community port depending on the secondary VLAN it is associated with.
promiscuous	Configures an interface as a private VLAN promiscuous port. The promiscuous ports are members of the primary VLAN.

Default general

Mode Interface Config

no switchport mode private-vlan

This command removes the private-VLAN association or mapping from the port.

Format no switchport mode private-vlan

Mode Interface Config

3.2.5.3. *Private-vlan*

This command configures the private VLANs and configures the association between the primary private VLAN and secondary VLANs.

Format private-vlan {association [add|remove] <secondary-vlanlist> | community | isolated | primary}

Parameter	Definition
association	Associates the primary and secondary VLAN.
secondary-vlan-list	A list of secondary VLANs to be mapped to a primary VLAN.
community	Designates a VLAN as a community VLAN.
isolated	Designates a VLAN as the isolated VLAN.
primary	Designates a VLAN as the primary VLAN.

Mode VLAN Config

no private-vlan

This command restores normal VLAN configuration.

Format no private-vlan [association]

Mode VLAN Config

3.2.6. Switch Ports

This section describes the commands used for switch port mode.

3.2.6.1. *Switchport mode access*

This command configures an interface to be operated on VLAN access mode. In this mode, only one VLAN could be assigned to this interface. Use 'switchport access vlan <vlan-id>' to configure the access VLAN. In VLAN access mode, only the untagged packets are handled.

Format switchport mode access

Default General Mode

Mode Interface Config

no switchport mode access

This command sets the mode to General.

Format no switchport mode access

Mode Interface Config

3.2.6.2. *Switchport trunk allowed vlan*

Use this command to configure the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. The default is all.

The VLANs list can be modified using the add or remove options or replaced with another list using the vlan-list, all, or except options. If all is chosen, all VLANs are added to the list of allowed vlan. The except option provides an exclusion list.

Trunk ports accept tagged packets, where tagged packets are processed on the VLAN ID contained in the packet, if this VLAN is in the allowed VLAN list. Tagged packets received with a VLAN ID to which the port is not a member are discarded and MAC learning is not performed. If a VLAN is added to the system after a port is set to the Trunk mode and it is in the allowed VLAN list, this VLAN is assigned to this port automatically.

Format switchport trunk allowed vlan {<vlan-list> | all | add <vlan-list> | remove <vlan-list> | except <vlan-list>}

Parameter	Definition
All	Specifies all VLANs from 1 to 4093. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
add	Adds the defined list of VLANs to those currently set instead of replacing the list.
remove	Removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4093; extended-range VLAN IDs of the form XY or X, Y, Z are valid in this command.
except	Lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.)
vlan-list	Either a single VLAN number from 1 to 4093 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

Default All

Mode Interface Config

no switchport trunk allowed vlan

This command resets the list of allowed VLANs on the trunk port to its default value.

Format no switchport trunk allowed vlan

Mode Interface Config

3.2.6.3. *Switchport trunk native vlan*

Use this command to configure the Trunk port Native VLAN (PVID) parameter. Any ingress untagged packets on the port are tagged with the value of Native VLAN. Native VLAN must be in the allowed VLAN list for tagging of received untagged packets. Otherwise, untagged packets are discarded. Packets marked with Native VLAN are transmitted untagged from Trunk port. The default is 1.

Format switchport trunk native vlan <vlan-id>

Default 1 (Default VLAN)

Mode Interface Config

no switchport trunk native vlan

Use this command to reset the switch port trunk mode native VLAN to its default value.

Format no switchport trunk native vlan

Mode Interface Config

3.2.6.4. *Switchport access vlan*

Use this command to configure the VLAN on the Access port. Only one VLAN can be assigned to the Access port. Access ports are members of VLAN 1 by default. Access ports may be assigned to a VLAN other than VLAN 1. Removing the Access VLAN on the switch makes the Access port a member of VLAN 1. Configuring an Access port to be a member of a VLAN that does not exist results in an error and does not change the configuration.

Format switchport access vlan <vlan-id>

Default 1 (Default VLAN)

Mode Interface Config

no switchport access vlan

This command sets the access VLAN ID to 1.

Format no switchport access vlan

Mode Interface Config

3.2.6.5. *Show interfaces switchport*

Use this command to display the switchport status for all interfaces or a specified interface.

Format show interfaces switchport [<slot/port> | port-channel <trunk-id>]

Mode Privileged EXEC

3.2.7. IGMP snooping commands

This section describes the commands which are used to configure IGMP Snooping.

IGMP snooping is designed to prevent flooding multicast traffic which can cause unnecessary load on host devices.

Note: IGMP Snooping can be enabled with MLAG. The configuration of IGMP Snooping on peers of MLAG must be the same to guarantee that MLAG can work correctly.

3.2.7.1. *set igmp*

Use this command to enable IGMP snooping globally.

Format set igmp

Default Disable

Mode Global Config

no set igmp

Use this command to disable IGMP snooping globally.

Format no set igmp

Mode Global Config

3.2.7.2. *Clear igmpsnooping*

Use this command to delete all dynamic entries in Multicast Forwarding Database which is managed by the IGMP Snooping.

Format clear igmpsnooping

Default None

Mode Privileged Exec

3.2.7.3. *Set igmp fast-leave*

Use this command to enable IGMP snooping fast-leave admin mode on one particular interface or all interfaces.

Format set igmp fast-leave <vlan id>

Default Disable

Mode vlan database

no set igmp fast-leave

Use this command to disable IGMP snooping fast-leave admin mode on one particular interface or all interfaces.

Format no set igmp fast-leave <vlan id>

Mode vlan database

3.2.7.4. *set igmp groupmembership-interval*

Use this command to configure IGMP Group Membership Interval time on one particular interface or all interfaces.

Format set igmp groupmembership-interval <vlan id> <2-3600>

Default 260

Mode Global Config
vlan database

no set igmp groupmembership-interval

Use this command to restore IGMP Group Membership Interval time to default value.

Format no set igmp groupmembership-interval <vlan id>

Mode Global Config
Vlan database

3.2.7.5. *set igmp mcrtrexpiretime*

Use this command to configure Multicast Router Present Expiration time globally or on one particular interface.

Format set igmp mcrtrexpiretime <vlan id> <0-3600>

Default 0

Mode Global Config

Vlan database

no set igmp mcrtrexpiretime

Use this command to restore Multicast Router Present Expiration time to default value.

Format no set igmp mcrtrexpiretime

Mode Global Config

vlan database

3.2.7.6. *set igmp mrouter*

Use this command to configure one particular interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format set igmp mrouter {<vlan-id>}

Default Disable

Mode Interface Config

no set igmp mrouter

Use this command to disable multicast router attached mode for one particular interface or a VLAN.

Format no ip igmp snooping mrouter { <vlan-id>}

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Interface Config

3.2.7.7. *Set igmp maxresponse*

Use this command to configure IGMP Maximum Response time on a particular VLAN.

Format set igmp maxresponse <vlan-id> <1-25>

Default 10

Mode Global Config

VLAN database

no set igmp maxresponse

Use this command to restore IGMP Maximum Response time on a particular VLAN to default value.

Format no set igmp maxresponse <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

VLAN database

3.2.7.8. *Set igmp report-suppression*

Use this command to enable Report Suppression one a particular VLAN.

Format set igmp report-suppression <vlan-id>

Default Disable

Mode VLAN database

no set igmp report-suppression

Use this command to disable Report Suppression on a particular VLAN.

Format no set igmp report-suppression <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode VLAN database

3.2.7.9. *Show igmp snooping*

Use this command to display IGMP snooping information.

Format show ip igmp snooping [vlan <vlan-id>]

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)

Mode Privilege Exec

Display Message

If no parameters are specified, this command displays the following information:

term	Definition
Admin Mode	Indicates whether or not IGMP Snooping is active on the switch.
Multicast Control Frame Count	The number of multicast control frames that are processed by the CPU
IGMP header validation	
VLANs enabled for IGMP snooping	The list of VLANS on which IGMP Snooping is enabled

If parameter <vlan-id> is specified, the following information appears:

Term	Definition
VLAN ID	VLAN Id
IGMP Snooping Admin Mode	Indicates whether IGMP Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether IGMP Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the

	VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Shows the amount of time in seconds that a switch will wait after receive IGMP Leave Packet.
Multicast Router Expiry Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.
Report Suppression Mode	Indicate whether Report Suppression mode is active on the VLAN.

3.2.7.10. *Show ip igmp snooping mrouter vlan*

Use this command to display information about statically configured multicast router-attached interfaces.

Format show ip igmp snooping mrouter vlan {[interface] <slot/port> | vlan-id>}

Parameter	Description
Interface slot/port	Interface number
vlan-id	Vlan number. The range of vlan id is 1 to 4093

Mode Privilege Exec

Display Message

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

3.2.7.11. *Show mac-address-table igmpsnooping*

Use this command to display the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format show mac-address-table igmpsnooping

Mode Privilege Exec

Display Message

Term	Definition
VLAN ID	The VLAN ID used with the MAC address to fully identify the L2Mcast Group packets
MAC Address	A multicast MAC address for which the switch has forwarding or filtering interfaces. The format is 01:00:5e:xx:xx:xx.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.

Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

3.2.8. IGMP snooping querier commands

This section describes the commands which are used to configure IGMP Snooping querier.

3.2.8.1. *Set igmp querier*

Use this command to enable IGMP snooping querier admin mode.

Format set igmp querier [vlan id]

Default Disable

Mode Global Config

Vlan database

no set igmp querier

Use this command to disable IGMP snooping querier admin mode.

Format no set igmp querier <vlan id>

Mode Global Config

Vlan database

3.2.8.2. *Set igmp querier address*

Use this command to configure IGMP snooping querier address.

Format set igmp querier <vlan id> address <ip-address>

Default 0.0.0.0

Mode Global Config

Vlan database

no set igmp querier address

Use this command to restore IGMP snooping querier address to default value.

Format no set igmp querier <vlan id> address

Mode Global Config

Vlan database

3.2.8.3. *Set igmp querier query-interval*

Use this command to configure IGMP snooping querier query interval.

Format set igmp querier query-interval <1-1800>

Default 60

Mode Global Config

no set igmp querier query-interval

Use this command to restore IGMP snooping querier query interval to default value.

Format no set igmp querier query-interval

Mode Global Config

3.2.8.4. *set igmp querier timer expiry*

Use this command to configure IGMP snooping querier querier expiry interval.

Format set igmp querier timer expiry <60-300>

Default 125

Mode Global Config

no set igmp querier timer expiry

Use this command to restore IGMP snooping querier querier expiry interval to default value.

Format no set igmp querier timer expiry

Mode Global Config

3.2.8.5. *set igmp querier version*

Use this command to configure IGMP snooping querier version.

Format set igmp querier version <1-3>

Default 2

Mode Global Config

no set igmp querier version

Use this command to restore IGMP snooping querier version to default value.

Format no set igmp querier version

Mode Global Config

3.2.8.6. *set igmp querier election participate*

Use this command to enable IGMP snooping querier vlan election participate mode.

Format set igmp querier election participate <vlan-id>

Default Disable

Mode vlan database

no set igmp querier election participate

Use this command to disable IGMP snooping querier vlan election participate mode.

Format no ip igmp snooping querier vlan election participate <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode vlan database

3.2.8.7. *Show igmpsnooping querier*

Use this command to display IGMP snooping querier global information.

Format show igmpsnooping querier

Display Message

Term	Definition
IGMP Snooping Querier Mode	Administrative mode for IGMP Snooping. The default is disable.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 125.

Mode Privilege Exec

3.2.8.8. *Show igmpsnooping querier vlan*

Use this command to display IGMP snooping querier vlan information.

Format show igmpsnooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Privilege Exec

Display Message

Term	Definition
IGMP Snooping Querier Vlan Mode	Display the administrative mode for IGMP Snooping for the switch.

Querier Election Participation Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Vlan Address	Displays the Snooping Querier Address to be used as source address in periodic IGMP queries sent on the specified VLAN.
Operational State	Specifies the operational state of the IGMP Snooping Querier on a VLAN.
Operational Version	Displays the operational IGMP protocol version of the querier.

3.2.8.9. *Show igmpsnooping querier detail*

Use this command to dsplay all of IGMP snooping querier information.

Format show igmpsnooping querier detail

Display Message

Term	Definition
IGMP Snooping Querier Mode	Administrative mode for IGMP Snooping. The default is disable.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic IGMP queries. This address is used when no address is configured on the VLAN on which query is being sent.
IGMP Version	Specify the IGMP protocol version used in periodic IGMP queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

Mode Privilege Exec

3.2.9. MLD Snooping Commands

3.2.9.1. *Show mldsnooping*

Use this command to display mld snooping information.

Format show ipv6 mldsnooping [interface { vlan <vlan-id>]

Parameter	Description
vlan-id	The VLAN ID. (Range: 1-4093)

Mode Privilege Exec

Display Message

If no parameters are specified, following information is displayed.

Term	Definition
Admin Mode	Indicates whether or not MLD Snooping is active on the switch.
Multicast Control Frame Count	Displays the number of MLD Control frames that are processed by the CPU.
VLANs enabled for MLD snooping	VLANs on which MLD Snooping is enabled

If parameter <vlan-id> is specified, following information appears.

Term	Definition
VLAN ID	VLAN ID.
MLD Snooping Admin Mode	Indicates whether MLD Snooping is active on the VLAN.
Fast Leave Mode	Indicates whether MLD Snooping Fast Leave is active on the VLAN.
Group Membership Interval	Shows the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface, which is participating in the VLAN, before deleting the interface from the entry. This value may be configured.
Max Response Time	Shows the amount of time in seconds that a switch will wait after receive MLD Leave Packet.
Multicast Router Expiry Time	Displays the amount of time to wait before removing an interface that is participating in the VLAN from the list of interfaces with multicast routers attached. The interface is removed if a query is not received. This value may be configured.

3.2.9.2. *Show ipv6 mld snooping mrouter vlan*

Use this command to display information about statically configured multicast router-attached interfaces.

Format show ipv6 mld snooping mrouter vlan {interface <slot/port>}

Parameter	Description
Interface <slot/port>	Interface number
Vlan id	Vlan number. The range of vlan id is 1 to 4093.

Mode Privilege Exec

Display Message

Term	Definition
Interface	Shows the interface on which multicast router information is being displayed.
VLAN ID	Displays the list of VLANs of which the interface is a member.

3.2.9.3. *Show mac-address-table mldsnooping*

Use this command to display the MLD Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format show mac-address-table mldsnooping

Mode Privilege Exec

Display Message

Term	Definition
MAC Address	A multicast MAC address for which the switch has forwarding or filtering information. The format is twodigit hexadecimal numbers that are separated by colons, for example 33:33:45:67:89:AB.
Type	The type of entry, which is either static (added by the user) or dynamic (added to the table as a result of a learning process or protocol.)
Description	The text description of this multicast table entry.
Interfaces	The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

3.2.9.4. *set mld*

Use this command to enable MLD Snooping globally.

Format set mld <vlan id>

Default Disable

Mode Global Config

Vlan database

no set mld

Use this command to disable MLD Snooping globally.

Format no set mld <vlan id>

Mode Global Config

Vlan database

3.2.9.5. *Clear mldsnooping*

Use this command to delete all dynamic entries in Multicast Forwarding Database which is managed by the MLD Snooping.

Format clear mldsnooping

Default None

Mode Privilege Exec

3.2.9.6. *Set mld fast-leave*

Use this command to enable MLD Snooping fast-leave admin mode on a particular interface or all interfaces.

Format set mld fast-leave <vlan id>

Default Disable

Mode Global Config
Vlan database

no set mld fast-leave

Use this command to disable MLD Snooping fast-leave admin mode on a particular interface or all interfaces.

Format no set mld fast-leave <vlan id>

Mode Global Config
vlan database

3.2.9.7. *set mld groupmembership-interval*

Use this command to configure the MLD Group Membership Interval time on a particular interface or all interfaces.

Format set mld groupmembership-interval <vlan id> <2-3600>

Default 260

Mode Global Config
Vlan database

no set mld groupmembership-interval

Use this command to restore the MLD Group Membership Interval time to default value.

Format no set mld groupmember-shipinterval <vlan id>

Mode Global Config
Vlan database

3.2.9.8. *set mld mcrtexpiretime*

Use this command to configure the Multicast Router Present Expiration time for the system or on a particular interface.

Format set mld mcrtrexpiretime <vlan id> <0-3600>

Default 0

Mode Global Config
vlan database

no set mld mcrtrexpiretime

Use this command to restore the Multicast Router Present Expiration time to default value.

Format no **set** mld mcrtrexpiretime <vlan id>

Mode Global Config
Vlan database

3.2.9.9. *set mld mrouter*

Use this command to configure the interface as a multicast router-attached interface or configure the VLAN ID for the VLAN that has the multicast router attached mode enabled.

Format set mld mrouter <vlan-id>

Default None

Mode Interface Config

no set mld mrouter

Use this command to disable multicast router attached mode for the interface or a VLAN.

Format no set mld mrouter <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Interface Config

3.2.9.10. *Set mld max-response-time*

Use this command to configure the MLD Maximum Response time on a particular VLAN.

Format set mld max-response-time <vlan-id> <1-65>

Default 10

Mode Global Config

VLAN database

no set mld max-response-time

Use this command to restore the MLD Maximum Response time on a particular VLAN to default value.

Format no set mld max-response-time <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

VLAN database

3.2.10. MLD Snooping Querier Commands

This section describes the commands which are used to configure MLD Snooping querier.

3.2.10.1. *Show mldsnooing querier*

Use this command to display MLD snooping querier global information.

Format show mldsnooping querier

Mode Privileged Exec

Display Message

Term	Definition
MLD Snooping Querier Mode	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
MLD Version	Specify the MLD protocol version used in periodic MLD queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 125.

3.2.10.2. *Show mldsnooping querier vlan*

Use this command to display MLD snooping querier vlan information.

Format show mldsnooping querier vlan <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Privileged Exec

Display Message

Term	Definition

MLD Snooping Querier Vlan Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Election Participation Mode	Displays the querier election participate mode on the VLAN. When this mode is disabled, up on seeing a query of the same version in the vlan, the snooping querier move to non querier state. Only when this mode is enabled, the snooping querier will participate in querier election where in the least ip address will win the querier election and operates as the querier in that VLAN. The other querier moves to non-querier state.
Querier Vlan Address	Displays the Snooping Querier Address to be used as source address in periodic MLD queries sent on the specified VLAN.
Operational State	Specifies the operational state of the MLD Snooping Querier on a VLAN.
Operational Version	Displays the operational MLD protocol version of the querier.

3.2.10.3. *Show mldsnooping querier detail*

Use this command to display MLD snooping querier global information.

Format show mldsnooping querier detail

Mode Privileged Exec

Display Message

Term	Definition
MLD Snooping Querier Mode	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
Querier Address	Specify the Snooping Querier Address to be used as source address in periodic MLD queries. This address is used when no address is configured on the VLAN on which query is being sent.
MLD Version	Specify the MLD protocol version used in periodic MLD queries.
Querier Query Interval	Specify the time interval in seconds between periodic queries sent by the snooping querier. The Query Interval must be a value in the range of 1 and 1800. The default value is 60.
Querier Expiry Interval	Specify the time interval in seconds after which the last querier information is removed. The Querier Expiry Interval must be a value in the range of 60 and 300. The default value is 120.

3.2.10.4. *set mld querier*

Use this command to enable MLD snooping querier admin mode.

Format set mld querier <vlan id>

Default Disable

Mode Global Config

Vlan database

no set mld querier

Use this command to disable MLD snooping querier admin mode.

Format no set mld querier <vlan id>

Mode Global Config

Vlan database

3.2.10.5. *set mld querier address*

Use this command to configure MLD snooping querier address.

Format set mld querier <vlan id> address <ipv6-address>

Default 0

Mode Global Config

Vlan database

no set mld querier address

Use this command to restore MLD snooping querier address to default value.

Format no set mld querier <vlan id> address

Mode Global Config

Vlan database

3.2.10.6. *set mld querier query-interval*

Use this command to configure MLD snooping querier querier interval.

Format set mld querier querier-interval <1-1800>

Default 60

Mode Global Config

no set mld querier querier-interval

Format no set mld querier querier-interval

Mode Global Config

3.2.10.7. *Set mld querier timer expiry*

Use this command to configure MLD snooping querier querier expiry interval.

Format set mld querier timer expiry <60-300>

Default 120

Mode Global Config

no set mld querier timer expiry

Use this command to restore MLD snooping querier querier expiry interval to default value.

Format no set mld querier timer expiry

Mode Global Config

3.2.10.8. *set mld querier election participate*

Use this command to enable MLD snooping querier vlan election participate mode.

Format set mld querier election participate <vlan-id>

Default Disable

Mode vlan database

no set mld querier election participate

Use this command to disable MLD snooping querier vlan election participate mode.

Format no set mld querier election participate <vlan-id>

Parameter	Description
<vlan-id>	The VLAN ID. (Range: 1-4093)

Mode Global Config

3.2.11. Port-Channel/LAG (802.3ad) Commands

This section describes the commands you use to configure port-channels, which is defined in the 802.3ad specification, and that are also known as link aggregation groups (LAGs). Link aggregation allows you to combine multiple full-duplex Ethernet links into a single logical link. Network devices treat the aggregation as if it were a single link, which increases fault tolerance and provides load sharing. The LAG feature initially load shares traffic based upon the source and destination MAC address. Assign the port-channel (LAG) VLAN membership after you create a port-channel. If you do not assign VLAN membership, the port-channel might become a member of the management VLAN which can result in learning and switching issues.

A port-channel (LAG) interface can be either static or dynamic, but not both. All members of a port channel must participate in the same protocols. A static port-channel interface does not require a partner system to be able to aggregate its member ports.

Note: If you configure the maximum number of dynamic port-channels (LAGs) that your platform supports, additional port-channels that you configure are automatically static.

3.2.11.1. *port-channel*

This command configures a new port-channel (LAG) and generates a logical *slot/port* number for the port-channel. The `name` field is a character string which allows the dash "-" character as well as alphanumeric characters. Use the `show port channel` command to display the `slot/port` number for the logical interface. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Note: Before you include a port in a port-channel, set the port physical mode. For more information

Format `port-channel name`

Mode Global Config

⋮

3.2.11.2. *addport*

This command adds one port to the port-channel (LAG). The first interface is a logical *unit/slot/port* number of a configured port-channel. You can add a range of ports by specifying the port range when you enter Interface Config mode (for example: `interface 1/0/1-1/0/4`. Instead of *unit/slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Note: Before adding a port to a port-channel, set the physical mode of the port. For more information

Format `addport` *logical slot/port*

Mode Interface Config

3.2.11.3. *deleteport (interface config)*

This command deletes a port or a range of ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel (or range of port-channels). Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format `deleteport` *logical slot/port*

Mode interface Config

3.2.11.4. *deleteport (global config)*

This command deletes all configured ports from the port-channel (LAG). The interface is a logical *unit/slot/port* number of a configured port-channel. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number

Format `deleteport {`*logical slot/port* `| all}`

Mode Global Config

3.2.11.5. *lacp actor admin state longtimeout*

Use this command to set LACP actor admin state to longtimeout.

Format `lacp actor admin state longtimeout`

Mode Interface Config

Note: This command is applicable only to physical interfaces.

no lacp actor admin state longtimeout

Use this command to set the LACP actor admin state to short timeout .

Format `no lacp actor admin state longtimeout`

Mode nterface Config

Note: This command is applicable only to physical interfaces.

3.2.11.6. *Lacp actor admin state passive*

Use this command to set the LACP actor admin state to passive.

Format `lacp actor admin state passive`

Mode Interface Config

Note: This command is applicable only to physical interfaces

no lacp actor admin state passive

Use this command to set the LACP actor admin state to active

Format `no lacp actor admin state passive`

Mode Interface Config

3.2.11.7. *lacp actor port priority*

Use this command to configure the priority value assigned to the Aggregation Port for an interface or range of interfaces. The valid range for *priority* is 0 to 65535.

Format `lacp actor port priority 0-65535`

Default 0x80

Mode Interface Config

N**ote:** This command is applicable only to physical interfaces.

no lacp actor port priority

Use this command to configure the default priority value assigned to the Aggregation Port

Format `no lacp actor port priority`

Mode Interface Config

3.2.11.8. *interface lag*

Use this command to enter Interface configuration mode for the specified LAG.

Format `interface lag lag-interface-number`

Mode Global Config

3.2.11.9. *Port Lacpmode*

This command enables Link Aggregation Control Protocol (LACP) on a port or range of ports.

Format `port lacpmode`

Default enabled

Mode Interface Config

No port lacpmode

This command disables Link Aggregation Control Protocol (LACP) on a port.

Format no port lacpmode

Mode Interface Config

3.2.11.10. *Port Lacpmode enable all*

This command enables Link Aggregation Control Protocol (LACP) on all ports.

Format `port lacpmode enable all`

Mode Global Config

no port lacpmode enable all

This command disables Link Aggregation Control Protocol (LACP) on all ports.

Format `no port lacpmode enable all`

Mode Global Config

3.2.11.11. *Port lacptimeout (interface config)*

This command sets the timeout on a physical interface or range of interfaces of a particular device type (actor or partner) to either long or short timeout.

Format `port lacptimeout {actor | partner} {long | short}`

Default long

Mode Interface Config

no port lacptimeout

This command sets the timeout back to its default value on a physical interface of a particular device type (actor or partner)

Format `no port lacptimeout {actor | partner}`

Mode Interface Config

Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the
ports. Consequently, both commands will display in `show running-config`.

3.2.11.12. *Port lacptimeout (global config)*

This command sets the timeout for all interfaces of a particular device type (actor or partner) to either long or short timeout.

Format `port lacptimeout {actor | partner} {long | short}`

Default long

Mode global Config

no port lacptimeout

This command sets the timeout for all physical interfaces of a particular device type (actor or partner) back to their default values

Format `no port lacptimeout {actor | partner}`

Mode Global Config

Note: Both the `no portlacptimeout` and the `no lacp actor admin state` commands set the values back to default, regardless of the command used to configure the ports. Consequently, both commands will display in `show running-config`

3.2.11.13. *Port-channel adminmode*

This command enables all configured port-channels with the same administrative mode setting

Format `port-channel adminmode all`

Mode global Config

no port-channel adminmode

This command disables all configured port-channels with the same administrative mode setting.

Format `no port-channel adminmode all`

Mode Global Config

3.2.11.14. *port-channel linktrap*

This command enables link trap notifications for the port-channel (LAG). The interface is a logical *unit/slot/ port* for a configured port-channel. The option `all` sets every configured port-channel with the same
administrative mode setting. Instead of *unit/slot/port*, `lag lag-intf-num` can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Note: This command is applicable only to physical interfaces

Format `port-channel linktrap {`*logical slot/port* `| lag | all}`

Default enabled

Mode global Config

No port-channel linktrap

This command disables link trap notifications for the port-channel (LAG). The interface is a logical slot and port for a configured port-channel. The option `all` sets every configured port-channel with the same administrative mode setting.

Format no `port-channel linktrap {`*logical slot/port* `| lag | all}`

Mode global Config

3.2.11.15. *Port-channel load-balance*

This command selects the load-balancing option used on a port-channel (LAG). Traffic is balanced on a port- channel (LAG) by selecting one of the links in the channel over which to transmit specific packets. The link is selected by creating a binary pattern from selected fields in a packet, and associating that pattern with a particular link.

Load-balancing is not supported on every device. The range of options for load-balancing may vary per device. This command can be configured for a single interface, a range of interfaces, or all interfaces. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number

Format `port-channel load-balance {1 | 2 | 3 | 4 | 5 | 6 } {`*slot/port* `| all}`

Default 3

Mode global Config

Term	*Definition*
1	Source MAC, VLAN, EtherType, and incoming port associated with the packet
2	Destination MAC, VLAN, EtherType, and incoming port associated with the packet
3	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet
4	Source IP and Source TCP/UDP fields of the packet
5	Destination IP and Destination TCP/UDP Port fields of the packet
6	Source/Destination IP and source/destination TCP/UDP Port fields of the packet
slot/port| all	Global Config Mode only: The interface is a logical slot/port number of a config

no port-channel load-balance

This command reverts to the default load balancing configuration.

Format `no port-channel load-balance {slot/port | all}`

Mode global Config

Term	*Definition*
slot/ port **| all**	Global Config Mode only: The interface is a logical *slot/port* number of a configured port-channel. **All** applies the command to all currently configured port- channels.

3.2.11.16. *Port-channel name*

This command defines a name for the port-channel (LAG). The interface is a logical *slot/port* for a configured port-channel, and *name* is an alphanumeric string up to 15 characters. Instead

of *unit/slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format port-channel name {*logical slot/port*} *name*

Mode global Config

3.2.11.17. *port-channel system priority*

Use this command to configure port-channel system priority. The valid range of *priority* is 0-65535.

Format port-channel system priority *priority*

Default 0x8000

Mode Global Config

no port-channel system priority

Use this command to configure the default port-channel system priority value.

Format no port-channel system priority

Mode global Config

3.2.11.18. *show lacp actor*

Use this command to display LACP actor attributes. Instead of *slot/port*, lag *lag-intf-num* can be used as an alternate way to specify the LAG interface. lag *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number

Format show lacp actor {*slot/port*|all}

Mode Privileged EXEC

The following output parameters are displayed.

Parameter	*Description*
System Priority	The administrative value of the Key.
Actor Admin Key	The administrative value of the Key.
Port Priority	The priority value assigned to the Aggregation Port.
Admin State	The administrative values of the actor state as transmitted by the Actor in LACPDUs.

3.2.11.19. *Show lacp partner*

Use this command to display LACP partner attributes. Instead of *unit/slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format `show lacp actor {`*slot/port* `| all}`

Mode Privileged EXEC

Parameter	*Description*
System Priority	The administrative value of priority associated with the Partner's System ID.
System-ID	Represents the administrative value of the Aggregation Port's protocol Partner's System ID.
Admin Key	The administrative value of the Key for the protocol Partner.
Port Priority	The administrative value of the Key for protocol Partner.
Port-ID	The administrative value of the port number for the protocol Partner.
Admin State	The administrative values of the actor state for the protocol Partner.

The following output parameters are displayed.

3.2.11.20. *Show port-channel brief*

This command displays the static capability of all port-channel (LAG) interfaces on the device as well as a summary of individual port-channel interfaces. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number.

Format show port-channel brief

Mode User EXEC

Term	*Definition*
Logical Interface	The *unit/slot/port* of the logical interface.
Port-channel Name	The name of port-channel (LAG) interface.
Link-State	Shows whether the link is up or down.
Trap Flag	Shows whether trap flags are enabled or disabled.
Type	Shows whether the port-channel is statically or dynamically maintained.
Mbr Ports	The members of this port-channel.
Active Ports	The ports that are actively participating in the port-channel.

For each port-channel the following information is displayed

3.2.11.21. *Show port-channel*

This command displays an overview of all port-channels (LAGs) on the switch. Instead of *slot/port*, `lag` *lag-intf-num* can be used as an alternate way to specify the LAG interface. `lag` *lag-intf-num* can also be used to specify the LAG interface where *lag-intf-num* is the LAG port number

Format `show port-channel {`*slot/port* `|` `all}`

Mode
- Privileged EXEC

Term	*Definition*
Logical Interface	The valid slot/port number.
Port-Channel Name	The name of this port-channel (LAG). You may enter any string of up to 15 alphanumeric characters.
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Type	The status designating whether a particular port-channel (LAG) is statically or dynamically maintained. • **Static** - The port-channel is statically maintained. • **Dynamic** - The port-channel is dynamically maintained
Mbr Ports	A listing of the ports that are members of this port-channel (LAG), in unit/slot/port notation. There can be a maximum of eight ports assigned to a given port-channel (LAG).
Device Timeout	For each port, lists the timeout (long or short) for Device Type (actor or partner).
Port Speed	Speed of the port-channel port.

3.2.11.22. *Show port-channel system priority*

Use this command to display the port-channel system priority

Format `show port-channel system priority`

Mode Privileged EXEC

3.2.11.23. *Show port-channel counters*

Use this command to display port-channel counters for the specified port

Format `show port-channel` *`slot/port`* `counters`

Mode Privileged EXEC

Term	*Definition*
Local Interface	The valid slot/port number.
Channel Nam	The name of this port-channel (LAG).
Link State	Indicates whether the Link is up or down.
Admin Mode	May be enabled or disabled. The factory default is enabled.
Port Channel Flap Count	The number of times the port-channel was inactive.
Mbr Ports	The slot/port for the port member.
Mbr Flap Counters	The number of times a port member is inactive, either because the link is down, or the admin state is disabled

3.2.11.24. *Clear port-channel counters*

Use this command to clear and reset specified port-channel and member flap counters for the specified interface

Format `clear port-channel {lag-intf-num | slot/port} counters`

Mode `Privileged EXEC`

3.2.11.25. *Clear port-channel all counters*

Use this command to clear and reset all port-channel and member flap counters for the specified interface

Format `clear port-channel all counters`

Mode Privileged EXEC

3.2.12. Storm Control

This section describes the commands you use to configure storm control or display storm control information. A traffic storm is a condition that occurs when incoming packets flood the LAN, which creates performance degradation in the network. The Storm-Control feature protects against this condition.

3.2.12.1. *Show storm-control*

This command displays switch configuration information. If you do not use any of the optional parameters, this command displays global storm control configuration parameters:

- **Broadcast Storm Recovery Mode** may be enabled or disabled. The factory default is disabled.
- **802.3x Flow Control Mode** may be enabled or disabled. The factory default is disabled.

Use the `all` keyword to display the per-port configuration parameters for all interfaces or specify the *`slot/ port`* to display information about a specific interface.

Format show storm-control [{ <slot/port> | all }]

Parameter	Definition
<slot/port>	Specifies a valid slot number and port number for the system.
all	Indicates to display the configuration parameters for all ports.

Mode Privileged EXEC

The following is the display format for the command without any optional parameter.

Display Message

Fields	Definition
Broadcast Storm Control Mode	The storm-control configuration mode for broadcast traffic.
Broadcast Storm Control Level	The storm-control speed threshold for broadcast traffic.
Broadcast Storm Control Action	The storm-control action for broadcast traffic.
Multicast Storm Control Mode	The storm-control configuration mode for multicast traffic.
Multicast Storm Control Level	The storm-control speed threshold for multicast traffic.
Multicast Storm Control Action	The storm-control action for multicast traffic.
Unicast Storm Control Mode	The storm-control configuration mode for unicast traffic.
Unicast Storm Control Level	The storm-control speed threshold for unicast traffic.
Unicast Storm Control Action	The storm-control action for unicast traffic.

The following is the display format for the command with a specific parameter.

Display Message

Fields	Definition
Intf	The interface number.
Bcast Mode	The storm-control configuration mode for broadcast traffic.
Bcast Level	The storm-control speed threshold for broadcast traffic.
Bcast Action	The storm-control action for broadcast traffic.
Mcast Mode	The storm-control configuration mode for multicast traffic.
Mcast Level	The storm-control speed threshold for multicast traffic.
Mcast Action	The storm-control action for multicast traffic.
Ucast Mode	The storm-control configuration mode for unicast traffic.
Ucast Level	The storm-control speed threshold for unicast traffic.
Ucast Action	The storm-control action for unicast traffic.
Flow Mode	The storm-control speed threshold for unicast traffic.

3.2.12.2. *Storm-control Configuration*

Use this command to enable storm control on each port or all ports.

Format storm-control {broadcast | multicast | unicast} [{action { shutdown| trap} | level <0-100>| rate <0-14880000>}]

Parameter	Definition
broadcast | multicast | unicast	Specifies to enable one of storm control modes for an interface or all interfaces.
action shutdown | trap	Indicates the action to be taken if the storm occurs. Shutdown is to disable the interface. Trap is to send SNMP trap.
level <0-100>	Specifies a threshold level (a percentage of link speed) for all interfaces or one interface. The default is 5.
rate <0-14880000>	Specifies a threshold rate(in packets per second) for all interfaces or one interface. The default is 0.

Default disabled

Mode Global Config
Interface Config

3.2.12.3. *Storm-control broadcast*

Use this command to enable broadcast storm control for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If the mode is enabled, broadcast storm recovery is active and, if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of broadcast traffic will be limited to the configured threshold.

Format storm-control broadcast

Default disabled

Mode Global Config
Interface Config

no storm-control broadcast

This command disables broadcast storm control for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control broadcast

Mode Global Config
Interface Config

3.2.12.4. *Storm-control broadcast action*

This command configures the broadcast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If configured to shutdown, the interface that receives the broadcast packets at a rate above the threshold is diagnostically disabled. If set to trap, the interface sends trap messages approximately every 30 seconds until broadcast storm control recovers.

Format storm-control broadcast action { shutdown | trap }

Default None

Mode Global Config
Interface Config

no storm-control broadcast action

This command configures the broadcast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control broadcast action

Mode Global Config
Interface Config

3.2.12.5. *Storm-control broadcast rate*

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second.

If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Format storm-control broadcast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

no storm-control broadcast rate

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery.

Format no storm-control broadcast rate

Mode Global Config
Interface Config

3.2.12.6. *Storm-control broadcast level*

Use this command to configure the broadcast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enable broadcast storm recovery.

If the mode is enabled, broadcast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of broadcast traffic is limited to the configured threshold.

Format storm-control broadcast level <0-100>

Default 5

Mode Global Config
Interface Config

no storm-control broadcast level

This command sets the broadcast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables broadcast storm recovery

Format no storm-control broadcast level

Mode Global Config
Interface Config

3.2.12.7. *Storm-control multicast*

This command enables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold.

Format storm-control multicast

Default disabled

Mode Global Config

Interface Config

no storm-control multicast

This command disables multicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control multicast

Mode Global Config
Interface Config

3.2.12.8. *Storm-control multicast action*

This command configures the multicast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If configured to shutdown, the interface that receives multicast packets at a rate above the threshold is diagnostically disabled. The option trap sends trap messages approximately every 30 seconds until multicast storm control recovers

Format storm-control multicast action {shutdown | trap}

Default None

Mode Global Config
Interface Config

no storm-control multicast action

This command returns the multicast storm recovery action option to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control multicast action

Mode Global Config
Interface Config

3.2.12.9. *Storm-control multicast level*

This command configures the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed and enables multicast storm recovery mode.

If the mode is enabled, multicast storm recovery is active, and if the rate of L2 multicast traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of multicast traffic will be limited to the configured threshold

Format storm-control multicast level <0-100>

Default 5

Mode Global Config
Interface Config

no storm-control multicast level

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format no storm-control multicast level

Mode Global Config
Interface Config

3.2.12.10. *Storm-control multicast rate*

Use this command to configure the multicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second.

If the mode is enabled, multicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped. Therefore, the rate of multicast traffic is limited to the configured threshold.

Format storm-control multicast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

no storm-control multicast rate

This command sets the multicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables multicast storm recovery.

Format no storm-control multicast rate

Mode Global Config
Interface Config

3.2.12.11. *Storm-control unicast*

This command enables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped. Therefore, the rate of unknown unicast traffic will be limited to the configured threshold.

Format storm-control unicast

Default disabled

Mode Global Config
Interface Config

no storm-control unicast

This command disables unicast storm recovery mode for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

Format no storm-control unicast

Mode Global Config
Interface Config

3.2.12.12. *Storm-control unicast action*

This command configures the unicast storm recovery action to either shutdown or trap for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode).

If configured to shutdown, the interface that receives unicast packets at a rate above the threshold is diagnostically disabled. The option trap sends trap messages approximately every 30 seconds until unicast storm control recovers.

Format storm-control unicast action { shutdown | trap }

Default None

Mode Global Config
Interface Config

no storm-control unicast action

This command returns the unicast storm recovery action option to the default value for all interfaces (GlobalConfig mode) or one or more interfaces (Interface Config mode).

Format no storm-control unicast action

Mode Global Config
Interface Config

3.2.12.13. *Storm-control unicast level*

This command configures the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) as a percentage of link speed, and enables unicast storm recovery.

If the mode is enabled, unicast storm recovery is active, and if the rate of unknown L2 unicast (destination lookup failure) traffic ingressing on an interface increases beyond the configured threshold, the traffic will be dropped.

Therefore, the rate of unknown unicast traffic will be limited to the configured threshold. This command also enables unicast storm recovery mode for an interface.

Format storm-control unicast level <0-100>

Default 5

Mode Global Config
Interface Config

no storm-control unicast level

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format no storm-control multicast level

Mode Global Config
Interface Config

3.2.12.14. *Storm-control unicast rate*

Use this command to configure the unicast storm recovery threshold for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) in packets per second.

If the mode is enabled, unicast storm recovery is active, and if the rate of L2 broadcast traffic ingressing on an interface increases beyond the configured threshold, the traffic is dropped.

Therefore, the rate of unicast traffic is limited to the configured threshold.

Format storm-control unicast rate <0-14880000>

Default 0

Mode Global Config
Interface Config

no storm-control unicast rate

This command sets the unicast storm recovery threshold to the default value for all interfaces (Global Config mode) or one or more interfaces (Interface Config mode) and disables unicast storm recovery.

Format no storm-control unicast rate

Mode Global Config
Interface Config

3.2.13. L2 Priority

3.2.13.1. *Show queue cos-map*

This command displays the class of service priority map on specific interface.

Format show queue cos-map <slot/port>

Parameter	Description
slot/port	Interface number .

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
User Priority	Displays the 802.1p priority to be mapped.
Traffic Class	Displays internal traffic class to map the corresponding 802.1p priority.

3.2.13.2. *Queue cos-map*

This command is used to assign class of service (CoS) value to the CoS priority queue.

Format queue cos-map <0-7> <0-7>

no queue cos-map

Parameter	Description
<0-7>	The range of queue priority is 0 to 7.
<0-7>	The range of mapped traffic class is 0 to 7.
no	Sets the CoS map to the default values

Default

priority	queue
0	1

1	0
2	0
3	1
4	2
5	2
6	3
7	3

Mode Interface Config

3.2.14. Port Mirror

This section describes the commands you use to select network traffic that you can analyze with a network analyzer.

Note: On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

3.2.14.1. *Show monitor session*

Use this command to display the port monitoring information for the specified session.

Format show monitor session { <1-4> | all }

Parameter	Definition
<1-4>	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions(4) allowed on the platform.
all	Displays the all sessions

Mode Privileged EXEC

Display Message

Term	*Definition*
Session ID	An integer value used to identify the session. Its value can be anything between 1 and the maximum number of mirroring sessions allowed on the platform.
Admin Mode	Indicates whether the Port Mirroring feature is enabled or disabled for the session identified with session-id. The possible values are Enabled and Disabled.
Probe Port	Probe port (destination port) for the session identified with session-id. If probe port is not set then this field is blank.
Remove RSPAN Tag	Remove RSPAN VLAN tag on the probe (destination) port. To configure this value probe port and remove RSPAN tag values should be specified simultaneously. If no probe port is configured for the session then this field is blank.
Mirrored Port(s)	The port that is configured as a mirrored port (source port) for the session identified with session-id. If no source port is configured for the session, this field is blank.
Session Type	The type of monitor session.
Source VLAN	All member ports of this VLAN are mirrored. If the source VLAN is not configured, this field is blank.
Reflector Port	This port carries all the mirrored traffic at the source switch.
Source RSPAN VLAN	The source VLAN configured at the destination switch. If remote VLAN is not configured, this field is blank
Destination RSPAN VLAN	The destination VLAN configured at the source switch. If remote VLAN is not configured, this field is blank
Source ERSPAN Flow ID	The ID number used by the source session to identify the ERSPAN traffic.
Destination ERSPAN Flow ID	The destination VLAN configured at the source switch. If remote VLAN is not configured, this field is blank
Source ERSPAN IP address	The ERSPAN flow destination IP address, which must be an address on a local interface and match the address entered in the ERSPAN destination session configuration.
Destination ERSPAN IP address	The ERSPAN flow destination IPv4 address , which must also be configured on an interface on the destination switch and be entered in the ERSPAN destination session configuration.
Destination ERSPAN Origin IP address	The IPv4 address used as the source of the ERSPAN traffic
Destination ERSPAN IP TTL	The IPv4 TTL value of the packets in the ERSPAN traffic.
Destination ERSPAN IP DSCP	The IP DSCP value of the packets in the ERSPAN traffic.

Destination ERSPAN IP Precedence	The IP precedence value of the packets in the ERSPAN traffic.
IP ACL	The IP access-list id or name attached to the port mirroring session.
MAC ACL	The MAC access-list name attached to the port mirroring session.

3.2.14.2. *monitor session source*

This command configures the source interface for a selected monitor session. Use the source interface slot/port parameter to specify the interface to monitor. Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note: The source and destination cannot be configured as remote on the same device. On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

Format monitor session <1-4> source { interface { <slot/port> | cpu | lag { <1-6> } } [{rx | tx}] } | remote vlan <1-4093>| vlan <1-4093> }

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4
<slot/port>	The Interface number
lag <1-6>	LAG interface number. The range of lag ID is 1 to 6.
rx | tx	Option rx is used to monitor only ingress packets. Option tx is used to monitor only egress packets. If no option is specified, both ingress and egress packets, RX and TX, are monitored.
remote vlan <1-4093>	The VLAN ID to be monitored on the remote switch. The range is 1 to 4093.
vlan <1-4093>	The VLAN ID to be monitored. The range is 1 to 4093.

Default None

Mode Global Config

no port-monitor session source

Use this command to remove the specified mirrored port from the selected port mirroring session.

Format no port-monitor session <session-id> source { interface {<slot/port> | cpu | lag } [{rx | tx} } | remote vlan <vlan-id>| vlan <vlan-id> }

Default None

Mode Global Config

3.2.14.3. *monitor session destination*

This command configures the probe interface for a selected monitor session. This command configures a probe port and a monitored port for monitor session (port monitoring).

Use rx to monitor only ingress packets, or use tx to monitor only egress packets. If you do not specify an {rx | tx} option, the destination port monitors both ingress and egress packets.

A VLAN can be configured as the source to a session (all member ports of that VLAN are monitored). Remote port mirroring is configured by adding the RSPAN VLAN ID. At the source switch, the destination is configured as the RSPAN VLAN and at the destination switch, the source is configured as the RSPAN VLAN.

Note: The source and destination cannot be configured as remote on the same device. On LY4R, one port cannot join more than one port-monitor session regardless of source port or destination port due to the HW limitation.

The reflector-port is configured at the source switch along with the destination RSPAN VLAN. The reflector port forwards the mirrored traffic towards the destination switch.

Note: This port must be configured with RSPAN VLAN membership.

Format port-monitor session <1-4> destination { interface <slot/port> | remote vlan <1-4093> reflector-port <slot/port> }

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4.
interface <slot/port>	The Interface number .
remote vlan <1-4093>	The VLAN ID to be monitored on the remote switch. The range is 1 to 4093.
reflector-port <slot/port>	The Interface number for reflector-port.

Default None

Mode Global Config

no monitor session destination

Use this command to remove the specified probe port from the selected port mirroring session.

Format no port-monitor session <session-id> destination { interface <slot/port> | remote vlan <vlan-id> reflector-port <slot/port> }

Default None

Mode Global Config

3.2.14.4. *monitor session mode*

Use this command to configure the mode parameters to enable the administrative mode of the selected port mirroring session. If enabled, the probe port monitors all the traffic received and transmitted on the physical monitored port.

Format port-monitor session <1-4> mode

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4.

Default None

Mode Global Config

no monitor session mode

The command disables port-monitoring function for the selected port monitoring session.

Format no port-monitor session <session-id> mode

Default None

Mode Global Config

3.2.14.5. *No monitor session*

Use this command without optional parameters to remove the monitor session (port monitoring) destination from the source probe port, the destination monitored port and all VLANs. Once the port is removed from the VLAN, you must manually add the port to any desired VLANs.

Format no port-monitor session <session-id>

Parameter	Definition
<1-4>	Session number. The range of session id is 1 to 4.

Default None

Mode Global Config

3.2.14.6. *No monitor*

This command removes all the source ports and a destination port and restores the default value for mirroring session mode for all the configured sessions.

Format no port-monitor

Default enabled

Mode Global Config

3.2.15. Link State

3.2.15.1. *Show link state*

Show link state information.

Format show link state group [<1-16>]

Parameter	Description
<1-16>	The range of group id is 1 to 16.

Default None

Mode Global Config

Display Message

Fields	Definition
Group ID	The group ID for each displayed row.
DownStream	Display such port was included to DownStream set.
UpStream	Display such port was included to UpStream set.
Link Action	This group was set which action
Group State	The state of this group

3.2.15.2. *Link state group action*

This command is used to Link DOWN the group downstream interface list when upstream link goes down (link is up otherwise) or Link UP the group downstream interface list when upstream link goes down (link is down otherwise).

Format link state group <1-16> action {down | up}

no link state group <1-16>

Parameter	Description
<1-16>	The range of group id is 1 to 16.
no	Disable the group action

Default None

Mode Global Config

3.2.15.3. *Link state group*

This command is used to add interface to the downstream/upstream interface list.

Format link state group <1-16> {downstream| upstream}

no link state group <1-16> {downstream| upstream}

Parameter	Description

<1-16>	The range of group id is 1 to 48.
no	Remove the selected interface from downstream/upstream list.

Default None

Mode Interface Config

3.3. Provisioning (IEEE 802.1p) Commands

This section describes the commands you use to configure provisioning (IEEE 802.1p,) which allows you to prioritize ports.

3.3.1. Vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface.

Format vlan priority <0-7>

Default 0

Mode Interface Config

no vlan priority

This command restores the priority configuration to default value.

Format no switchport priority

Mode Interface Config

3.4. Management Commands

3.4.1. Network Commands

3.4.1.1. *Show ip interface*

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format `show ip interface {slot/port|vlan 1-4093 }`

Default None

Mode Privileged Exec

Term	*Definition*
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

Display Message

3.4.1.2. *Mtu*

Use the mtu command to set the maximum transmission unit(MTU) size, in bytes, for frames that ingress or egress the interface. You can use the mtu command to configure jumbo frame support for physical and port-channel(LAG) interfaces. for the standard ICOS implementation, the MTU size is a valid integer between 1522-12288 for tagged packets and a valid integer between 1518-1228 for untagged packets.

Note: To receive and process packets, the Ethernet MTU must include any extra bytes that Layer-2 headers might require. To configure the IP MTU size, which is the maximum size of the IP packet(IP Header + IP payload).

Format mtu <1500-9198>

Default 1518(untagged)

Mode Interface Config

no mtu

This command sets the default MTU size(in bytes) for the interface.

Format no mtu

Mode Interface Config

3.4.1.3. *Interface vlan*

This command is used to create a vlan interface and enter Interface-vlan configuration mode.

Format interface vlan <vlan-id>

Parameter	Definition
<vlan-id>	VLAN ID (Range: 1 - 4093).

Default None

Mode Global Config

3.4.1.4. *Ip address*

This command configures an IP address on an interface or range of interfaces. You can also use this command to configure one or more secondary IP addresses on the interface. The command supports RFC 3021 and accepts using 31-bit prefixes on IPv4 point-to-point links. This command adds the label IP address in the command "show ip interface".

Format ip address <ipaddr> {subnetmask | /prefix-length} [secondary]

Parameter	Definition
ipaddr	The IP address of the interface.
subnetmask	A 4-digit dotted-decimal number which represents the subnet mask of the interface.
masklen	Implements RFC 3021. Using the/notation of the subnet mask, this is and integer that indicates the length of subnet mask. Range is 5 to 32 bits.

Default IP address: 0.0.0.0

Subnet Mask: 0.0.0.0

Mode Interface-Vlan Config

Example: The following example of the command shows the configuration of the subnet mask with an IP address in the dotted decimal format on interface vlan 100.

(Pakedge-MS-1212-189667) (interdace vlan 100)#ip address 192.168.10.2 255.255.255.254

(Pakedge-MS-1212-189667) (interdace vlan 100)#

no ip address

This command deletes an IP address from an interface. The value for ipaddr is the IP address of the interface in a.b.c.d format where the range for a,b,c, and d is 1-255. The value for subnetmask is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface. To remove all of the IP addresses(primary and secondary) configured on the interface, enter the command no ip address.

Format no ip address <ipaddr> {subnetmask | /prefix-length} [secondary]

Mode Interface-Vlan Config

3.4.1.5. *Ip default-gateway*

This command sets the IP Address of the default gateway.

Format ip default-gateway <gateway-addr>
no ip default-gateway

Parameter	Definition
< gateway-addr >	IP address of the default gateway.
no	Restore the default IP address of the default gateway.

Default IP address: 0.0.0.0

Mode Global Config

3.4.1.6. *Ip address dhcp*

This command specifies the network configuration protocol to be used. If you modify this value, the change is effective immediately.

Format ip address dhcp

Parameter	Definition
<dhcp>	Obtains IP address from DHCP.

Default None

Mode Interface-Vlan Config

3.4.2. Serial Interface Commands

3.4.2.1. *Show line console*

This command displays serial communication settings for the switch.

Format show line console

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Serial Port Login Timeout (minutes)	Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.
Baud Rate	The default baud rate at which the serial port will try to connect. The available values are 1200, 2400, 4800, 9600, 19200, 38400, 57600, and 115200 bauds.
Character Size	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The Parity Method used on the Serial Port. The Parity Method is always None.
Password Threshold	When the logon attempt threshold is reached on the console port, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the silent time command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface closes.
Silent Time (sec)	Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password threshold command.
Terminal Length	The columns per page for terminal serial port.

3.4.2.2. *Line console*

This command is used to enter Line configuration mode

Format line console

Default None

Mode Global Config

3.4.2.3. *Serial Baudrate*

This command specifies the communication rate of the terminal interface. The supported rates are 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200.

Format serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600 | 115200}

Default 115200

Mode Line Config

no serial baudrate

This command sets the communication rate of the terminal interface to **115200**.

Format no serial baudrate

Mode Line Config

3.4.2.4. *Serial timeout*

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Format serial timeout <0-160>

Default 5

Mode Line Config

no serial timeout

This command sets the maximum connect time (in minutes) without console activity to 5.

Format no serial timeout

Mode Line Config

3.4.2.5. *show serial*

This command displays serial communication settings for the switch.

Format `show serial`

Term	*Definition*
Serial Port Login Timeout (minutes)	The time, in minutes, of inactivity on a serial port connection, after which the switch will close the connection. A value of 0 disables the timeout.
Baud Rate (bps)	The default baud rate at which the serial port will try to connect.
Character Size (bits)	The number of bits in a character. The number of bits is always 8.
Flow Control	Whether Hardware Flow-Control is enabled or disabled. Hardware Flow Control is always disabled.
Stop Bits	The number of Stop bits per character. The number of Stop bits is always 1.
Parity	The parity method used on the Serial Port. The Parity Method is always None.

Mode Privileged Exec

3.4.3. Telnet Session Commands

3.4.3.1. *telnet*

This command establishes a new outbound telnet connection to a remote host.

Format telnet <ip-address|hostname> [port] [debug] [line]

Parameter	Definition
<ip-address|hostname>	A hostname or a valid IPv4 address.
port	A valid decimal integer in the range of 0 to 65535, where the default value is 23.
debug	Display current enabled telnet options.
line	Set the outbound telnet operational mode as 'linemode', where by default, the operational mode is 'character mode'.

Default None

Mode Privileged Exec

User Exec

3.4.3.2. *Show telnetcon*

This command displays telnet settings.

Format show telnetcon

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Remote Connection Login Timeout (minutes)	This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. A zero means there will be no timeout. May be specified as a number from 0 to 160. The factory default is 5.
Maximum Number of Remote Connection Sessions	This object indicates the number of simultaneous remote connection sessions allowed. The factory default is 5.
Allow New Telnet Sessions	Indicates that new telnet sessions will not be allowed when set to no. The factory default value is yes.
Telnet Server Admin Mode	The telnet server admin mode status. The factory default is enable.
Telnet Server Port	The configured TCP port number on which the Telnet server listens for requests.

3.4.3.3. *Line telnet*

This command is used to enter vty (Telnet) configuration mode.

Format line telnet

Default None

Mode Global Config

3.4.3.4. *transport input telnet*

This command enables/disables telnet server. If telnet server is enabled, all telnet sessions can be established until there are no more sessions available. If telnet server is disabled, all telnet sessions are closed.

Format transport input telnet

Default Enabled

Mode Line Vty

no transport input telnet

Format no transport input telnet

Mode Line Vty

3.4.3.5. *telnetcon maxsessions*

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

Format telnetcon maxsessions <0-4>

Default 4

Mode Global Config

no telnetcon maxsessions

This command sets the maximum value to be 54

Format no telnetcon maxsessions

Mode Global Config

3.4.3.6. *telnetcon timeout*

This command sets the outbound telnet session timeout value in minute.

Changing the timeout value for active sessions does not become effective until the session is reaccessed. Any keystroke will also activate the new timeout duration.

Format telnetcon timeout <1-160>

Default 5

Mode Global Config

no telnetcon timeout

This command sets the remote connection session timeout value, in minutes, to the default.

Format no telnetcon timeout

Mode Global Config

3.4.3.7. *show telnet*

This command displays the current outbound telnet settings.

Format show telnet

Default None

Mode Privileged Exec
User Exec

Display Message

Parameter	Definition
Outbound Telnet Login Timeout (in minutes)	Indicates the number of minutes an outbound telnet session is allowed to remain inactive before being logged off. A value of 0, which is the default, results in no timeout.
Maximum Number of Outbound Telnet Sessions	Indicates the number of simultaneous outbound telnet connections allowed.
Allow New Outbound Telnet Sessions	Indicates whether outbound telnet sessions will be allowed.

3.4.4. SNMP Server Commands

3.4.4.1. Show snmp

This command displays SNMP community information and SNMP trap/inform receivers. Trap/Inform messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network.

You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.

The SNMP agent of the switch complies with SNMP versions 1, 2c, and 3 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format show snmp

Default None

Mode Privileged EXEC

Display Message

Parameter	Definition
Community-String	The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 20 characters. Each row of this table must contain a unique community name.
Community-Access	The access level for this community string.
View Name	The view this community has access to.
IP Address	Access to this community is limited to this IP address.
Group Name	The community this mapping configures.
Target Address	An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community.
Type	The type of message that will be sent, either traps or informs.
Community	The community traps will be sent to.
Version	The version of SNMP the trap will be sent as.
SNMP v1	Uses SNMP v1 to send traps to the receiver.
SNMP v2	Uses SNMP v2 to send traps to the receiver.
SNMP v3	Uses SNMP v3 to send traps to the receiver.
UDP Port	The UDP port the trap or inform will be sent to.
Filter name	The filter the traps will be limited by for this host.
TO Sec	The number of seconds before informs will time out when sending to this host.
Retries	The number of times informs will be sent after timing out.

Username	The user this mapping configures.
Security Level	The authentication and encryption level for snmpv3.
NoAuth-N	No authentication checksum and no encryption algorithm assigned.
Auth-NoP	Md5 or sha authentication checksum assigned and no encryption algorithm assigned.
Auth-Pri	Md5 or sha authentication checksum and des encryption algorithm assigned.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp

Community-String Community-Access View Name IP Address

---------- ---------- --------- ------- ---------- ----------

private Read/Write Default All

public Read Only Default All

Community-String Group Name IP Address

---------- ---------- ----------

private DefaultWrite All

public DefaultRead All

Traps are enabled.

Authentication trap is enabled.

Version 1,2 notifications

Target Address Type Community Version UDP Filter TO Retries

Port

name Sec

---------- -------- ---------- ---------- ------- -------- ----- ------

10.1.1.1 Trap public 2 123 test

Version 3 notifications

Target Address Type Username Security UDP Filter TO Retries

Level Port

name Sec

--- --- --- --- --- --- --- ---

10.2.2.2 Inform test NoAuth-N 162 300 255

System Contact:

System Location:

3.4.4.2. Snmp-server sysname

This command sets the name of the switch. The range for name is from 1 to 64 alphanumeric characters.

Format snmp-server sysname <name>

Parameter	Definition
<name>	Range is from 1 to 64 alphanumeric characters.

Default None

Mode Global Config

3.4.4.3. Snmp-server location

This command sets the physical location of the switch. The range for name is from 1 to 255 alphanumeric characters.

Format snmp-server location <loc>

Parameter	Definition
<loc>	Range is from 1 to 255 alphanumeric characters.

Default None

Mode Global Config

3.4.4.4. Snmp-server contact

This command sets the organization responsible for the network. The range for contact is from 1 to 255 alphanumeric characters.

Format snmp-server contact <con>

Parameter	Definition
<con>	Range is from 1 to 255 alphanumeric characters.

Default None

Mode Global Config

3.4.4.5. Snmp-server community

This command adds a new SNMP community, and optionally sets the access mode, allowed IP address, and creates a view for the community. The allowed IP address supports IPv4 and IPv6 address but does not support IP mask value to demote a range of IPv6 addresses.

Note: Community names in the SNMP community table must be unique. If you make multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Format snmp-server community <community-string> [ipaddress <ipaddress> | ro | rw | su | view <viewname>]

Parameter	Definition
<Community-String>	A name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of community-name can be up to 20 case-sensitive characters.
ipaddress	The associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses.
ro | rw | su	The access mode of the SNMP community, which can be public (Read-

	Only/RO), private (Read-Write/RW), or Super User (SU).
<viewname>	The name of the view to create or update.

Default None

Mode Global Config

no snmp-server community <community-string>

This command deletes snmp community.

Format no snmp-server community <community-string>

Mode Global Config

3.4.4.6. Snmp-server community-group

This command configures a community access string to permit access via the SNMPv1 and SNMPv2c protocols.

Format snmp-server community-group <community-string> <group-name> [ipaddress <ip-address>]

Parameter	Definition
<community-string>	The community which is created and then associated with the group. The range is 1 to 20 characters.
<group-name>	The name of the group that the community is associated with. The range is 1 to 30 characters.
<ip-address>	Optionally, the IPv4 address that the community may be accessed from.

Default None

Mode Global Config

no snmp-server community-group <community-string>

This command deletes snmp community group.

Format no snmp-server community-group <community-string>

Mode Global Config

3.4.4.7. Show snmp engineid

This command displays the currently configured SNMP engineID.

Format show snmp engineid

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Local SNMP EngineID	The current configuration of the displayed SNMP engineID.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp engineid

Local SNMP engineID : 80001c4c032c600c83ad47

3.4.4.8. Snmp-server engineID

This command configures snmp engineID on the local device.

Note: Changing the engineID will invalidate all SNMP configuration that exists on the box.

Format snmp-server engineID local {<engine-id> | default}

Parameter	Definition
<engine-id>	A hexadecimal string identifying the engine-id. Engine-id must be an even length in the range of 6 to 32 hexadecimal characters.
default	Sets the engine-id to the default string, based on the device MAC address.

Default The engineID is configured automatically, based on the device MAC address.

Mode Global Config

no snmp-server engineID

This command removes snmp engineID.

Format no snmp-server engineID local

Mode Global Config

3.4.4.9. Show snmp filters

This command displays the configured filters used when sending traps.

Format show snmp filters [<filter-name>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Name	The filter name for this entry.
OID Tree	The OID tree this entry will include or exclude.
Type	Indicates if this entry includes or excludes the OID Tree.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp filters

Name	OID Tree	Type
test	fastPathSwitching	Included

3.4.4.10. Snmp-server filter

This command creates a filter entry for use in limiting which traps will be sent to a host.

Format snmp-server filter <filter-name> <oid-tree> [excluded | included]

Parameter	Definition

<filter-name>	The label for the filter being created. The range is 1 to 30 characters.
<oid-tree>	The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
excluded	The tree is excluded from the filter.
included	The tree is included in the filter.

Default None

Mode Global Config

no snmp-server filter <filter-name> [<oid-tree >]

This command removes the specified filter.

Format no snmp-server filter <filter-name> [<oid-tree >]

Mode Global Config

3.4.4.11. Show snmp user

This command displays the currently configured SNMPv3 users.

Format show snmp user [<username>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Name	The name of the user.
Group Name	The group that defines the SNMPv3 access parameters.
Auth Method	The authentication algorithm configured for this user.
Privilege Method	The encryption algorithm configured for this user.
Remote Engine ID	The engineID for the user defined on the client machine.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp user

Name	Group Name	Auth Meth	Priv Meth	Remote Engine ID
test	DefaultRead	MD5	DES	8000c95403e8c74f189667

3.4.4.12. Snmp-server user

This command creates an SNMPv3 user for access to the system.

Format snmp-server user <name> <group-name> [remote <engine-idstring>] {[auth-md5 <password> | auth-md5-key <md5-key> | auth-sha <password> | auth-sha-key <sha-key>] [priv-des <password> | priv-des-key <des-key>]}

Parameter	Definition
<name>	The username the SNMPv3 user will connect to the switch as. The range is 1 to 30 characters.
<group-name>	The name of the group the user belongs to. The range is 1 to 30 characters.
<engineid-string>	The engine-id of the remote management station that this user will be connecting from. The range is 6 to 32 characters.
<password>	The password the user will use for the authentication or encryption mechanism. The range is 8 to 32 characters.
md5-key	A pregenerated MD5 authentication key. The length is 32 characters.
sha-key	A pregenerated SHA authentication key. The length is 48 characters.
priv-des-key	A pregenerated DES encryption key. The length is 32 characters.

Default None

Mode Global Config

no snmp-server user

This command removes the specified SNMPv3 user.

Format no snmp-server user <name> [remote <engine-idstring>]

Mode Global Config

3.4.4.13. Show snmp group

This command displays the configured groups.

Format show snmp group [<groupname>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Name	The name of the group.
Security Model	Indicates which protocol can access the system via this group.
Security Level	Indicates the security level allowed for this group.
Read View	The view this group provides read access to.
Write View	The view this group provides write access to.
Notify View	The view this group provides trap access to.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp group

Name	Context Prefix	Security Model	Security Level	Views Read	Write	Notify
DefaultRead	""	V1	NoAuth-NoPriv	Default	""	Default

DefaultRead "" V2 NoAuth-NoPriv Default ""
Default

DefaultRead "" V3 NoAuth-NoPriv Default ""
Default

DefaultRead "" V3 Auth-NoPriv Default ""
Default

DefaultRead "" V3 Auth-Priv Default ""
Default

DefaultSuper "" V1 NoAuth-NoPriv DefaultS DefaultS DefaultS

uper uper uper

DefaultSuper "" V2 NoAuth-NoPriv DefaultS DefaultS DefaultS

uper uper uper

DefaultSuper "" V3 NoAuth-NoPriv DefaultS DefaultS DefaultS

uper uper uper

DefaultWrite "" V1 NoAuth-NoPriv Default Default Default

DefaultWrite "" V2 NoAuth-NoPriv Default Default Default

DefaultWrite "" V3 NoAuth-NoPriv Default Default Default

DefaultWrite "" V3 Auth-NoPriv Default Default Default

DefaultWrite "" V3 Auth-Priv Default Default Default

3.4.4.14. Snmp-server group

This command creates an SNMP access group.

Format snmp-server group <group-name> [v1 | v2 | v3 {auth | noauth | priv}] {[read <readview>] | [write <writeview>] | [context <contextprefix>] | [notify <notifyview>]}

Parameter	Definition
<group-name>	The group name to be used when configuring communities or users. The range is 1 to 30 characters.

v1	This group can only access via SNMPv1.
v2	This group can only access via SNMPv2c.
v3	This group can only access via SNMPv3.
<readview>	The view this group will use during GET requests. The range is 1 to 30 characters.
<writeview>	The view this group will use during SET requests. The range is 1 to 30 characters.
<notifyview>	The view this group will use when sending out traps. The range is 1 to 30 characters.

Default Generic groups are created for all versions and privileges using the default views.

Mode Global Config

no snmp-server group

This command removes the specified group.

Format no snmp-server group <group-name> [v1 | v2 | v3 {auth | noauth | priv}] { [context <contextprefix>] | [notify <notifyview>]}

Mode Global Config

3.4.4.15. Show snmp views

This command displays the currently configured views.

Format show snmp views [<viewname>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Name	The view name for this entry.
OID Tree	The OID tree that this entry will include or exclude.

Type	Indicates if this entry includes or excludes the OID tree.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp views

Name	OID Tree	Type
Default	iso	Included
Default	snmpVacmMIB	Excluded
Default	usmUser	Excluded
Default	snmpCommunityTable	Excluded
DefaultSuper	iso	Included

3.4.4.16. Snmp-server view

This command creates or modifies an existing view entry that is used by groups to determine which objects can be accessed by a community or user.

Format snmp-server view <view-name> <oid-tree> [excluded | included]

Parameter	Definition
<view-name>	The label for the view being created. The range is 1 to 30 characters.
<oid-tree>	The OID subtree to include or exclude from the filter. Subtrees may be specified by numerical (1.3.6.2.4) or keywords (system), and asterisks may be used to specify a subtree family (1.3.*.4).
excluded	The tree is excluded from the view.
included	The tree is included in the view.

Default Views are created by default to provide access to the default groups.

Mode Global Config

no snmp-server view

This command removes the specified view.

Format no snmp-server view <view-name> [<oid-tree>]

Mode Global Config

3.4.5. SNMP Trap Commands

3.4.5.1. Snmp-server host <host-addr> traps

This command configures traps to be sent to the specified host.

Format snmp-server host <host-addr> traps version {1 <community> | 2 <community> | 3 <username> [auth | noauth | priv]} [filter <filtername>] [udp-port <1-65535>]

Parameter	Definition
<host-addr>	The IPv4 or IPv6 address of the host to send the trap to.
version 1	Sends SNMPv1 traps.
version 2	Sends SNMPv2 traps.
<community>	Community string sent as part of the notification. The range is 1 to 20 characters.
version 3	Sends SNMPv3 traps.
<username>	Username of SNMPv3.
auth	Enables authentication of a packet without encrypting.
noauth	Disables authentication and encrypting of a packet.
priv	Enables authentication and encrypting of a packet.
<filtername>	The filter name to associate with this host. Filters can be used to specify which traps are sent to this host. The range is 1 to 30 characters.
<udp-port>	The SNMP trap receiver port. The default is port 162.

Default None

Mode Global Config

no snmp-server host <host-addr>

This command deletes trap receivers.

Format no snmp-server host <host-addr>

Mode Global Config

3.4.5.2. Show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format show trapflags

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Authentication Flag	May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.
Link Up/Down Flag	May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.
Multiple Users Flag	May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).
Spanning Tree Flag	May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.
ACL Traps	May be enabled or disabled. The factory default is disabled. Indicates whether ACL traps will be sent.
BGP Traps	May be enabled or disabled. The factory default is disabled. Indicates whether BGP traps will be sent.
OSPFv2 Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPF traps will be sent.
PIM Traps	May be enabled or disabled. The factory default is disabled. Indicates whether PIM traps will be sent.
OSPFv3 Traps	May be enabled or disabled. The factory default is disabled. Indicates whether OSPFv3 traps will be sent.
Power Supply Module state trap	May be enabled or disabled. The factory default is enabled. Indicates whether power supply status traps will be sent.
Temperature trap	May be enabled or disabled. The factory default is enabled. Indicates whether temperature status traps will be sent.

Fan trap	May be enabled or disabled. The factory default is enabled. Indicates whether fan status traps will be sent.
FIP snooping Traps	May be enabled or disabled. The factory default is enabled. Indicates whether snooping traps will be sent.
Transceiver Traps	May be enabled or disabled. The factory default is disabled. Indicates whether Transceiver traps will be sent.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show trapflags

Authentication Flag..... Enable

Link Up/Down Flag..... Enable

Multiple Users Flag..... Enable

Spanning Tree Flag..... Enable

ACL Traps..... Disable

BGP Traps..... Disable

OSPFv2 traps..... Disable

PIM Traps..... Disable

OSPFv3 Traps..... Disable

Power Supply Module state trap..... Enable

Temperature trap..... Enable

Fan trap..... Enable

FIP snooping Traps..... Enable

Transceiver Flag..... Disable

3.4.5.3. Snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled. See 'snmp-server enable traps linkmode‘ command.

Format snmp trap link-status all

Default Disabled

Mode Global Config

no snmp trap link-status all

This command disables link status traps for all interfaces.

Format no snmp trap link-status all

Mode Global Config

3.4.5.4. Snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see 'snmp trap link-status' command).

Format snmp-server enable traps linkmode

Default Enabled

Mode Global Config

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format no snmp-server enable traps linkmode

Mode Global Config

3.4.5.5. Snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 or telnet) and there is an existing terminal interface session.

Format snmp-server enable traps multiusers

Default Enabled

Mode Global Config

no snmp-server enable traps multiusers

This command disables Multiple User trap.

Format no snmp-server enable traps multiusers

Mode Global Config

3.4.5.6. Snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Format snmp-server enable traps stpmode

Default Enabled

Mode Global Config

no snmp-server enable traps stpmode

This command disables the sending of new root traps and topology change notification traps.

Format no snmp-server enable traps stpmode

Mode Global Config

3.4.5.7. Snmp-server enable traps violation

This command enables the violation trap.

Format snmp-server enable traps violation

Default Disabled

Mode Global Config

no snmp-server enable traps violation

This command disables the violation trap.

Format no snmp-server enable traps violation

Mode Global Config

3.4.5.8. Show snmp source-interface

This command displays the configured global source interface used for the SNMP client. The IP address of the selected interface is used as source IP for all communications with the server.

Format show snmp source-interface

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
SNMP trap Client Source Interface	The interface configured as the source interface for the SNMP trap/inform client.
SNMP trap Client IPv4 Address	The IP address configured on the SNMP client source interface.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show snmp source-interface

SNMP trap Client Source Interface..... 0/1
SNMP trap Client Source IPv4 Address..... 172.16.3.60 [Up]
SNMP trap Client Source IPv6 Address..... fe80::2f61:cff:fe83:ad47 [Up]

3.4.5.9. Snmptrap source-interface

Use this command in Global configuration mode to configure the global source-interface (Source IP address) for all SNMP communications between the SNMP client and the server. This command takes effect for both SNMP trap and inform client.

Format snmptrap source-interface {<slot/port> | vlan <vlan-id>}

Parameter	Definition
<slot/port>	Specifies the interface to use as the source interface.
<vlan-id>	Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default Disabled

Mode Global Config

no snmptrap source-interface

This command removes the global source-interface for all SNMP communication between the SNMP client and the server.

Format no snmptrap source-interface

Mode Global Config

3.4.6. SNMP Inform Commands

3.4.6.1. Snmp-server host <host-addr> informs

This command configures informs to be sent to the specified host.

Format snmp-server host <host-addr> informs version {2 <community> | 3 <username> [auth | noauth | priv]} [filter <filtername>] [udp-port <1-65535>] [retries <0-255>] [timeout <1-300>]

Parameter	Definition
<host-addr>	The IPv4 or IPv6 address of the host to send the inform to.
version 2	Sends SNMPv2 informs.
<community>	Community string sent as part of the notification. The range is 1 to 20 characters.
version 3	Sends SNMPv3 informs.
<username>	Username of SNMPv3.

auth	Enables authentication of a packet without encrypting.
noauth	Disables authentication and encrypting of a packet.
priv	Enables authentication and encrypting of a packet.
<filtername>	The filter name to associate with this host. Filters can be used to specify which informs are sent to this host. The range is 1 to 30 characters.
<udp-port>	The SNMP Inform receiver port. The default is port 162.
<retries>	The number of times to resend an Inform. The default is 3 attempts. The range is 0 to 255 retries.
<timeout>	The number of seconds to wait for an acknowledgement before resending the Inform. The default is 15 seconds. The range is 1 to 300 seconds.

Default None

Mode Global Config

no snmp-server host <host-addr>

This command deletes inform receivers.

Format no snmp-server host <host-addr>

Mode Global Config

3.4.7. Secure Shell (SSH) Commands

3.4.7.1. *Show ip ssh*

This command displays the SSH settings.

Format show ip ssh

Default None

Mode Privileged Exec

Display Message

Parameter	Definition

Administrative Mode	This field indicates whether the administrative mode of SSH is enabled or disabled.
SSH Port	The listen port number of SSH service.
Protocol Levels	The protocol level supports.
SSH Sessions Currently Active	This field specifies the current number of SSH connections.
Max SSH Sessions Allowed	The maximum number of inbound SSH sessions allowed on the switch.
SSH Timeout	This field is the inactive timeout value for incoming SSH sessions to the switch.
Keys Present	Indicates whether the SSH RSA and DSA key files are present on the device.
Key Generation in Progress	Indicates whether RSA or DSA key files generation is currently in progress.
User Password Authentication	Indicates whether the SSH authentication mode of user password is enabled or disabled.
User Public Key Authentication	Indicates whether the SSH authentication mode of user public key is enabled or disabled.
Terminal Length	indicates the number of lines to be paginated and displayed on a screen for a new SSH session.

3.4.7.2. *Ip ssh*

This command is used to enable SSH.

Format ip ssh

Default Enabled

Mode Global Config

no ip ssh

This command is used to disable SSH.

Format no ip ssh

Mode Global Config

3.4.7.3. *sshcon maxsessions*

This command specifies the maximum number of SSH connection sessions that can be established. A value of 0 indicates that no ssh connection can be established. The range is 0 to 5.

Format ip ssh maxsessions <0-2>

Default 2

Mode Global Config

no sshcon maxsessions

This command sets the maximum number of SSH connection sessions that can be established to the default value.

Format no ip ssh maxsessions

Mode Global Config

3.4.7.4. *sshcon timeout*

This command specifies the maximum idle time for each SSH login session. The range is 1 to 160 minutes.

Format sshcon timeout <1-160>

Default 5

Mode Global Config

no sshcon timeout

This command sets the maximum idle time for each SSH login session to the default value.

Format no sshcon timeout

Mode Global Config

3.4.8. Management Security Commands

3.4.8.1. *Crypto key generation {RSA|DSA}*

This command is used to generate an RSA or DSA key pair for SSH. Please note that the SSHv1 key will not be generated.

Format crypto key generate {RSA | DSA}

Default None

Mode Global Config

no crypto key generate {RSA | DSA}

This command is used to delete the RSA or DSA key from the device.

Format no crypto key generate {RSA | DSA}

Mode Global Config

3.4.8.2. *Crypto certificate generation*

This command is used to generate a certificate for HTTPS.

Format crypto certificate generate

Default None

Mode Global Config

no crypto certificate generate

This command is used to delete the certificate from the device.

Format no crypto certificate generate

Mode Global Config

3.4.9. Time Range Commands

3.4.9.1. *Show time-range*

Use this command to display a time range and all the absolute/periodic time entries that are defined for the time range. Use the name parameter to identify a specific time range to display. When name is not specified, all the time ranges defined in the system are displayed.

Format show time-range [<name>]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Number of Time Ranges	Number of time ranges configured in the system.
Time Range Name	Name of the time range.
Time Range Status	Status of the time range (active/inactive).
Absolute start	Start time and day for absolute time entry.
Absolute end	End time and day for absolute time entry.
Periodic Entries	Number of periodic entries in a time-range.
Periodic start	Start time and day for periodic entry.
Periodic end	End time and day for periodic entry.

3.4.9.2. *Time-range*

Use this command to enable or disable the time range Admin mode.

Format time-range

Default None

Mode Global Config

no time-range

This command sets the time-range Admin mode to disable.

Format no time-range

Mode Global Config

3.4.9.3. *Time-range <name>*

Use this command to create a time range identified by name, consisting of one absolute time entry and/or one or more periodic time entries. The name parameter is a case-sensitive, alphanumeric string from 1 to 31 characters that uniquely identifies the time range. An alpha-numeric string is defined as consisting of only alphabetic, numeric, dash, underscore, or space characters.

If a time range by this name already exists, this command enters Time-Range config mode to allow updating the time range entries

Format time-range <name>

Parameter	Definition
<name>	time range name.

Default None

Mode Global Config

no time-range <name>

This command deletes a time-range identified by name.

Format no time-range <name>

Mode Global Config

3.4.9.4. *Absolute*

Use this command to add an absolute time entry to a time range. Only one absolute time entry is allowed per time-range. The time parameter is based on the currently configured time zone.

The [start time date] parameters indicate the time and date at which the configuration that referenced the time range starts going into effect. The time is expressed in a 24-hour clock, in the form of hours:minutes. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

The date is expressed in the format day month year. If no start time and date are specified, the configuration statement is in effect immediately.

The [end time date] parameters indicate the time and date at which the configuration that referenced the time range is no longer in effect. The end time and date must be after the start time and date. If no end time and date are specified, the configuration statement is in effect indefinitely.

Format absolute {start <hh:mm> <1-31> <month> <1970-2035> [end <hh:mm> <1-31> <month> <1970-2035>] | end <hh:mm> <1-31> <month> <1970-2035>}

Default None

Mode Time-Range Config

no absolute

This command deletes the absolute time entry in the time range.

Format no absolute

Mode Time-Range Config

3.4.9.5. *Periodic*

Use this command to add a periodic time entry to a time range. The time parameter is based off of the currently configured time zone.

The first occurrence of the days-of-the-week argument is the starting day(s) from which the configuration that referenced the time range starts going into effect. The second occurrence is the ending day or days from which the configuration that referenced the time range is no longer in effect. If the end days-of-the-week are the same as the start, they can be omitted

This argument can be any single day or combinations of days: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, Sunday. Other possible values are:

- daily — Monday through Sunday
- weekdays — Monday through Friday
- weekend — Saturday and Sunday

If the ending days of the week are the same as the starting days of the week, they can be omitted. The first occurrence of the time argument is the starting hours:minutes which the configuration that referenced the time range starts going into effect. The second occurrence is the ending hours:minutes at which the configuration that referenced the time range is no longer in effect.

The hours:minutes are expressed in a 24-hour clock. For example, 8:00 is 8:00 am and 20:00 is 8:00 pm.

Format periodic {days-of-the-week time} to {[days-of-the-week] time}

Default None

Mode Time-Range Config

no periodic

This command deletes a periodic time entry from a time range.

Format no periodic {days-of-the-week time} to {[days-of-the-week] time}

Mode Time-Range Config

3.4.10. Switch Database Management Template Commands

A Switch Database Management (SDM) template is a description of the maximum resources a switch or router can use for various features. Different SDM templates allow different combinations of scaling factors, enabling different allocations of resources depending on how the device is used. In other words, SDM templates enable you to reallocate system resources to support a different mix of features based on your network requirements.

3.4.10.1. *Show sdm prefer*

Use this command to display the current active SDM template and its scaling parameters, or to display the scaling parameters for an inactive template. When invoked with no optional keywords, this command lists the current active template and the template that will become active on the next reboot if it is different from the current active template. To list the scaling parameters of a specific template, use that template's keyword as an argument to the command.

Format show sdm prefer { dual-ipv4-and-ipv6 {alpm | data-center | dcvpn-data-center | default} | ipv4-routing {data-center {default | plus} | dcvpn-data-center | default}}

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
dual-ipv4-and-ipv6 alpm	(Optional) Lists the scaling parameters for the alpm template.

dual-ipv4-and-ipv6 data-center	(Optional) Lists the scaling parameters for the Dual IPv4 and IPv6 template supporting more ECMP next hops.
dual-ipv4-and-ipv6 dcvpn-data-center	(Optional)Lists the scaling parameters for the Dual IPv4 and IPv6 template for the DCVPN feature.
dual-ipv4-and-ipv6 default	(Optional) Lists the scaling parameters for the template supporting IPv4 and IPv6.
ipv4-routing data-center default	(Optional) Lists the scaling parameters for the IPv4-only template supporting more ECMP next hops.
ipv4-routing data-center plus	(Optional) Lists the scaling parameters for the IPv4-only template maximizing the number of unicast routes and also supporting more ECMP next hops.
ipv4-routing dcvpn-data-center	(Optional) Lists the scaling parameters for the IPv4-only template for DCVPN feature.
ipv4-routing default	(Optional) Lists the scaling parameters for the IPv4-only template maximizing the number of unicast routes.

3.4.10.2. *Sdm Prefer*

Use this command to change the template that will be active after the next reboot.

Format sdm perfer {dual-ipv4-and-ipv6 {alpm | data-center | dcvpn-data-center | default} | ipv4-routing {data-center {default | plus}| dcvpn-data-center | default}}

Parameter	Definition
dual-ipv4-and-ipv6 alpm	Accommodate larger routes.
dual-ipv4-and-ipv6 data-center	Increase the number of ECMP next hops in each route to 32 and reduce the number of IPv4 and IPv6 unicast routes.
dual-ipv4-and-ipv6 dcvpn-data-center	Maximize the number of IPv4 and IPv6 unicast routes while supporting DCVPN feature.
dual-ipv4-and-ipv6 default	Maximize the number of IPv4 and IPv6 unicast routes while limiting the number of ECMP next hops in each route to 4.
ipv4-routing data-center default	Increase the number of ECMP next hops to 32 and reduce the number of IPv4 routes.
ipv4-routing data-center plus	Increase the number of ECMP next hops to 32 while keeping the maximum IPv4 routes.

ipv4-routing dcvpn-data-center	Maximize the number of IPv4 unicast routes while supporting DCVPN feature.
ipv4-routing default	Maximize the number of IPv4 unicast routes while limiting the number of ECMP next hops in each route to 4.

Default dual-ipv4-and-ipv6 data-center

Mode Global Config

no sdm prefer

This command reverts to the default template after the next reboot.

Format no sdm prefer

Mode Global Config

3.5. Spanning Tree Protocol Commands

This section describes the commands you use to configure Spanning Tree Protocol (STP). STP helps prevent network loops, duplicate messages, and network instability.

Note: STP is enabled on the switch and on all ports and LAGs by default.

Note: If STP is disabled, the system does not forward BPDU messages.

3.5.1. Show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree. The following details are displayed.

Format show spanning-tree

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
Bridge Priority	Specifies the bridge priority for the Common and Internal Spanning tree (CST). The value lies between 0 and 61440. It is displayed in multiples of 4096.

Bridge Identifier	The bridge identifier for the CST. It is made up using the bridge priority and the base MAC address of the bridge.
Time Since Topology Change	Time in seconds.
Topology Change Count	Number of times changed.
Topology Change in progress	Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.
Designated Root	The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.
Root Path Cost	Value of the Root Path Cost parameter for the common and internal spanning tree.

Parameter	Definition
Root Port Identifier	Identifier of the port to access the Designated Root for the CST
Bridge Max Age	Maximum message age.
Bridge Max Hops	The maximum number of hops for the spanning tree.
Max Tx Hold Count	The max value of bridge tx hold count for the spanning tree.
Bridge Forwarding Delay	A timeout value to be used by all Bridges in the Bridged LAN. The value of Forward Delay is set by the Root.
Hello Time	Configured value of the parameter for the CST.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).
CST Regional Root	Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.
Regional Root Path Cost	Path Cost to the CST Regional Root.

3.5.2. Show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

Format show spanning-tree interface {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
Hello Time	Admin hello time for this port.
Port Mode	Enabled or disabled.
Auto Edge	To enable or disable the feature that causes a port that has not seen a BPDU for edge delay time, to become an edge port and transition to forwarding faster.

Port Up Time Since Counters Last Cleared	Time since port was reset, displayed in days, hours, minutes, and seconds.
STP BPDUs Transmitted	Spanning Tree Protocol Bridge Protocol Data Units sent.
STP BPDUs Received	Spanning Tree Protocol Bridge Protocol Data Units received.
RSTP BPDUs Transmitted	Rapid Spanning Tree Protocol Bridge Protocol Data Units sent.
RSTP BPDUs Received	Rapid Spanning Tree Protocol Bridge Protocol Data Units received.
MSTP BPDUs Transmitted	Multiple Spanning Tree Protocol Bridge Protocol Data Units sent.
MSTP BPDUs Received	Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

3.5.3. Show spanning-tree mst detailed

This command displays the detailed settings for an MST instance. The instance <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Format show spanning-tree mst detailed <mstid>

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MST Instance ID	The multiple spanning tree instance ID.
MST Bridge Priority	The bridge priority of current MST.
MST Bridge Identifier	The bridge ID of current MST.
Time Since Topology Change	In seconds.
Topology Change Count	Number of times the topology has changed for this multiple spanning tree instance.
Topology Change in progress	Value of the Topology Change parameter for the multiple spanning tree instance.
Designated Root	Identifier of the Regional Root for this multiple spanning tree instance.
Root Path Cost	Path Cost to the Designated Root for this multiple spanning tree instance.
Root Port Identifier	Port to access the Designated Root for this multiple spanning tree instance.
Associated FIDs	List of forwarding database identifiers associated with this instance.
Associated VLANs	List of VLAN IDs associated with this instance.

3.5.4. Show spanning-tree mst summary

This command displays summary information about all multiple spanning tree instances in the switch. On execution, the following details are displayed.

Format show spanning-tree mst summary

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MST Instance ID List	List of multiple spanning trees IDs currently configured.
For each MSTID: • **Associated FIDs** • **Associated VLANs**	• List of forwarding database identifiers associated with this instance. • List of VLAN IDs associated with this instance.

3.5.5. Show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The parameter <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot/port> is the desired switch port.

Format show spanning-tree mst port detailed <mstid> {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MST Instance ID	The ID of the existing MST instance.
Port Identifier	The port identifier for the specified port within the selected MST instance. It is made up from the port priority and the interface number of the port.
Port Priority	The priority for a particular port within the selected MST instance. The port priority is displayed in multiples of 16.
Port Forwarding State	Current spanning tree state of this port.
Port Role	Each enabled MST Bridge Port receives a Port Role for each spanning tree. The port role is one of the following values: Root Port, Designated Port, Alternate Port, Backup Port, Master Port or Disabled Port.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled.
Port Path Cost	Configured value of the Internal Port Path Cost parameter.
Designated Root	The Identifier of the designated root for this port.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	Bridge Identifier of the bridge with the Designated Port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.

If you specify 0 (defined as the default CIST ID) as the mstid, this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The slot/port is the desired switch port. In this case, the following are displayed.

Parameter	Definition

Port Identifier	The port identifier for this port within the CST.
Port Priority	The priority of the port within the CST.
Port Forwarding State	The forwarding state of the port within the CST.
Port Role	The role of the specified interface within the CST.
Auto-Calculate Port Path Cost	Indicates whether auto calculation for port path cost is enabled or not (disabled).
Port Path Cost	The configured path cost for the specified interface.
Auto-Calculate External Port Path Cost	Indicates whether auto calculation for external port path cost is enabled.
External Port Path Cost	The cost to get to the root bridge of the CIST across the boundary of the region. This means that if the port is a boundary port for an MSTP region, then the external path cost is used.
Designated Root	Identifier of the designated root for this port within the CST.
Designated Port Cost	Path Cost offered to the LAN by the Designated Port.
Designated Bridge	The bridge containing the designated port.
Designated Port Identifier	Port on the Designated Bridge that offers the lowest cost to the LAN.
Topology Change Acknowledgement	Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.
Hello Time	The hello time in use for this port.
Edge Port	The configured value indicating if this port is an edge port.
Edge Port Status	The derived value of the edge port status. True if operating as an edge port; false otherwise.
Point To Point MAC Status	Derived value indicating if this port is part of a point to point link.
CST Regional Root	The regional root identifier in use for this port.
CST Internal Root Path Cost	The internal root path cost to the LAN by the designated external port.

3.5.6. Show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <mstid> indicates a particular MST instance. The <misted> range is 0 to 4096. The parameter <slot/port> indicates the desired switch port.

If you specify 0 (defined as the default CIST ID) as the mstid, the status summary displays for one or all ports within the common and internal spanning tree.

Format show spanning-tree mst port summary <mstid> [{<slot/port> | active | port-channel <portchannel-id>}]

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MST Instance ID	The MST instance associated with this port.
Interface	slot/port
STP Mode	Indicates whether spanning tree is enabled or disabled on the port.

Type	Currently not used.
STP State	The forwarding state of the port in the specified spanning tree instance.
Port Role	The role of the specified port within the spanning tree.
Desc	Indicates whether the port is in loop inconsistent state or not.

3.5.7. Show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format show spanning-tree summary

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
Spanning Tree Admin mode	Enabled or disabled.
Spanning Tree Version	Version of 802.1 currently supported (IEEE 802.1s, IEEE 802.1w, or IEEE 802.1d) based upon the Force Protocol Version parameter.
Configuration Name	Identifier used to identify the configuration currently being used.
Configuration Revision Level	Identifier used to identify the configuration currently being used.
Configuration Digest Key	A generated Key used in the exchange of the BPDUs.
Configuration Format Selector	Specifies the version of the configuration format being used in the exchange of BPDUs. The default value is zero.
MST Instances	List of all multiple spanning tree instances configured on the switch.

3.5.8. Show spanning-tree brief

This command displays spanning tree settings for the bridge. The following information appears.

Format show spanning-tree brief

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
Bridge Priority	Configured value.
Bridge Identifier	The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.
Bridge Max Age	Configured value.
Bridge Max Hops	Bridge max-hops count for the device.

Bridge Hello Time	Configured value.
Bridge Forward Delay	Configured value.
Bridge Hold Time	Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs).

3.5.9. Spanning-tree

This command sets the spanning-tree operational mode to enabled.

Note: **If the MST is enabled with MLAG, MST must be enabled on both MLAG peer devices.**

Format spanning-tree

Default Enabled

Mode Global Config

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format no spanning-tree

Mode Global Config

Mode Global Config

3.5.10. Spanning-tree bpdumigration

This command enables BPDU migration check on a given interface. The all option enables BPDU migration check on all interfaces.

Format spanning-tree bpdumigrationcheck{<slot/port> | port-channel <portchannel-id> | all}

Default None

Mode Global Config

3.5.11. Spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The name is a string of up to 32 characters.

Note: **If the MST is enabled with MLAG, the Configuration Identifier Name must be the same on both MLAG peer devices.**

Format spanning-tree configuration name <name>

Default Base MAC address in hexadecimal notation

Mode Global Config

no spanning-tree configuration name

This command sets the Configuration Identifier Name to “DEFAULT”.

Format no spanning-tree configuration name

Mode Global Config

3.5.12. Spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Format spanning-tree configuration revision <0-65535>

Default 0

Mode Global Config

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value.

Format no spanning-tree configuration revision

Mode Global Config

3.5.13. Spanning-tree mode

This command configures global spanning tree mode per VLAN spanning tree. On a switch, only one mode can be enabled at a time.

Note: Both RSTP and MSTP can be enabled with MLAG. The configuration of RSTP and MSTP on peers of MLAG must be the same to guarantee that MLAG can work correctly. If you configure one peer of MLAG as RSTP, the other peer must be RSTP. The same as MSTP.

Format spanning-tree mode {mstp | rstp}

Default mstp

Mode Global Config

no spanning-tree mode

This command globally configures the switch to the default spanning-tree mode, MSTP.

Format no spanning-tree mode

Mode Global Config

3.5.14. Spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to “(Bridge Max Age / 2) + 1”.

Format spanning-tree forward-time <4-30>

Default 15

Mode Global Config

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value.

Format no spanning-tree forward-time

Mode Global Config

3.5.15. Spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to “2 times (Bridge Forward Delay - 1)” and greater than or equal to “2 times (Bridge Hello Time + 1)”.

Format spanning-tree max-age <6-40>

Default 20

Mode Global Config

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value.

Format no spanning-tree max-age

Mode Global Config

3.5.16. Spanning-tree forward-time max-age

This command sets the Bridge Forward Delay and Max Age parameter to a new value for the common and internal spanning tree.

Format spanning-tree forward-time <4-30> max-age <6-40>

Default forward-time: 15
max-age: 20

Mode Global Config

3.5.17. Spanning-tree max-hops

This command sets the MSTP Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is a range from 6 to 40.

Format spanning-tree max-hops <6-40>

Default 20

Mode Global Config

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value.

Format no spanning-tree max-hops

Mode Global Config

3.5.18. Spanning-tree mst instance

This command adds a multiple spanning tree instance to the switch. The parameter mstid is a number within a range of 1 to 4094 that corresponds to the new instance ID to be added. The maximum number of multiple instances supported by the switch is 4.

Format spanning-tree mst instance <mstid>

Default None

Mode Global Config

no spanning-tree mst instance

This command removes a multiple spanning tree instance from the switch and reallocates all VLANs allocated to the deleted instance to the common and internal spanning tree. The parameter mstid is a number that corresponds to the desired existing multiple spanning tree instance to be removed.

Format no spanning-tree mst instance <mstid>

Mode Global Config

3.5.19. Spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The parameter mstid <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.

If you specify 0 (defined as the default CIST ID) as the mstid, this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value is a number within a range of 0 to 61440. The twelve least significant bits are masked according to the 802.1s specification. This causes the priority to be rounded down to the next lower valid priority.

Format spanning-tree mst priority <mstid> <0-61440>

Default 32768

Mode Global Config

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value. The parameter mstid <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance.

If 0 (defined as the default CIST ID) is passed as the mstid, this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value.

Format no spanning-tree mst priority <mstid>

Mode Global Config

3.5.20. Spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are no longer associated with the common and internal spanning tree. The parameter mstid <0-4094> is a number that corresponds to the desired existing multiple spanning tree instance. The vlan-list can be specified as a single VLAN, a list, or a range of values. To specify a list of VLANs, enter a list of VLAN IDs, each separated by a comma with no spaces in between. To specify a range of VLANs, separate the beginning and ending VLAN ID with a dash (-). The VLAN IDs may or may not exist in the system.

Format spanning-tree mst vlan <mstid> <vlan-list>

Mode Global Config

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and one or more VLANs so that the VLAN(s) are again associated with the common and internal spanning tree.

Format no spanning-tree mst vlan <mstid> <vlan-list>

Mode Global Config

3.5.21. Spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If you specify an mstid <0-4094> parameter that corresponds to an existing multiple spanning tree instance, the configurations are done for that multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the mstid, the configurations are done for the common and internal spanning tree instance.

If you specify the cost option, the command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter. You can set the path cost as a number in the range of 1 to 200000000 or auto. If you select auto the path cost value is set based on Link Speed.

If you specify the port-priority option, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Note: **If the MST is enabled with MLAG, the path cost of the MLAG peer-link cannot be modified.**

Format spanning-tree mst <mstid> {{cost <1-200000000> | auto} | port-priority <0-240>}

Default cost: auto
port-priority: 128

Mode Interface Config

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance, or in the common and internal spanning tree to the respective default values. If you specify an mstid parameter that corresponds to an existing multiple spanning tree instance, you are configuring that

multiple spanning tree instance. If you specify 0 (defined as the default CIST ID) as the mstid, you are configuring the common and internal spanning tree instance.

If you specify cost, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter, to the default value, i.e., a path cost value based on the Link Speed.

If you specify port-priority, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the mstid parameter, to the default value.

Format no spanning-tree mst <mstid> {cost | port-priority}

Mode Interface Config

3.5.22. Spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Format spanning-tree port mode

Default Enabled

Mode Interface Config

no spanning-tree port mode

This command sets the Administrative Switch Port State for this port to disabled.

Format no spanning-tree port mode

Mode Interface Config

3.5.23. Spanning-tree port model all

This command sets the Administrative Switch Port State for all ports to enabled.

Format spanning-tree port mode all

Default Enabled

Mode Global Config

no spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to disabled.

Format no spanning-tree port mode all

Mode Global Config

3.5.24. Spanning-tree auto-edge

Use this command to allow the interface to become an edge port if it does not receive any BPDUs within a given amount of time.

Format spanning-tree auto-edge

Default Enabled

Mode Interface Config

no spanning-tree auto-edge

This command resets the auto-edge status of the port to the default value.

Format no spanning-tree auto-edge

Mode Interface Config

3.5.25. Spanning-tree cost

Use this command to configure the external path cost for port used by a MST instance. When the auto keyword is used, the path cost from the port to the root bridge is automatically determined by the speed of the interface. To configure the cost manually, specify a cost value from 1 – 200000000.

Note: **If the MST is enabled with MLAG, the path cost of the MLAG peer-link cannot be modified.**

Format spanning-tree cost {<cost> | auto}

Default Auto

Mode Interface Config

no spanning-tree cost

This command resets the path cost to the default value.

Format no spanning-tree cost

Mode Interface Config

3.5.26. Spanning-tree edgeport

This command specifies that an interface is an Edge Port within the common and internal spanning tree. This allows this port to transition to Forwarding State without delay.

Format spanning-tree edgeport

Mode Interface Config

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format no spanning-tree edgeport

Mode Interface Config

3.5.27. Spanning-tree bpduguard

Use this command to enable BPDU Guard on an interface.

Format spanning-tree bpduguard

Default Disabled

Mode Global Config

no spanning-tree bpduguard

Use this command to disable BPDU Guard on the interface.

Format no spanning-tree bpduguard

Mode Interface Config

3.5.28. Spanning-tree guard

Use this command to select whether loop guard or root guard is enabled on an interface or range of interfaces.

Format spanning-tree guard {loop | root|none}

Parameter	Definition
loop	This command sets the Guard Mode to loop guard on this interface.
root	This command sets the Guard Mode to root guard on this interface.

Default Disabled

Mode Interface Config

no spanning-tree guard

Use this command to disable loop guard or root guard on the interface.

Format no spanning-tree guard

Mode Interface Config

3.5.29. Spanning-tree tcnguard

Use this command to enable TCN guard on the interface. When enabled, TCN guard restricts the interface from propagating any topology change information received through that interface.

Format spanning-tree tcnguard

Default Enabled

Mode Interface Config

no spanning-tree tcnguard

Use this command to reset the TCN guard status of the port to the default value.

Format no spanning-tree tcnguard

Mode Interface Config

3.6. System Log Commands

3.6.1. Show logging

This command displays configurations of logging application.

Format show logging

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show logging

Logging Client Local Port           : 514
Logging Client Source Interface     : (not configured)
CLI Command Logging                 : disabled
Console Logging                     : enabled
Console Logging Severity Filter     : error
Buffered Logging                    : enabled
Buffered Logging Severity Filter    : info
Persistent Logging                  : disabled
Persistent Logging Severity Filter  : alert

Syslog Logging                      : disabled
Syslog Logging Facility             : user

Terminal Monitor                    : disabled
Terminal Logging Severity Filter    : warning

Log Messages Received               : 139
Log Messages Dropped                : 0
Log Messages Relayed                : 0

(Pakedge-MS-1212-189667) #
```

3.6.2. Show logging buffered

This command displays the log messages which record system operating and tracing information. The log buffered messages store in memory, therefore, it isn't retained across a switch reset.

Format show logging buffered

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show logging buffered

Buffered (In-Memory) Logging        : enabled
Buffered Logging Wrapping Behavior  : On
Buffered Log Count                  : 33

Apr 28 19:35:09: %1-6-NIM: [396203556] nim_rif.c(352) 117 %% Set expandable port 0/50 count set
to 1
Apr 28 19:35:09: %1-6-NIM: [396203556] nim_rif.c(352) 116 %% Set expandable port 0/49 count set
to 1
Apr 28 19:35:05: %1-5-TRAPMGR: [397164180] traputil.c(797) 115 %% Temperature state change
alarm: Unit Number: 1 Current: Normal, Previous: None
Apr 28 19:34:59: %1-5-TRAPMGR: [396792620] traputil.c(755) 114 %% Succeeded User Login: Console
started for user admin connected from EIA-232.
Apr 28 19:34:57: %1-5-TRAPMGR: [396792620] traputil.c(755) 113 %% Entity Database: Configuration
Changed
Apr 28 19:34:52: %1-2-General: [1212183788] Boot!(0) 112 %% Event(0xaaaaaaaa)
Apr 28 19:34:52: %1-6-AUTO_INST: [1212183788] auto_install_control.c(1374) 111 %% AutoInstall is
stopped.
Apr 28 19:34:52: %1-5-SIM: [1212183788] sim_util.c(3841) 110 %% Switch firmware operational:
LY8, Runtime Code 5.4.01.10, Linux 3.8.13-rt9, U-Boot 2010.12 (Oct 03 2014 - 14:38:07) - ONIE
2014.05.03-7
Apr 28 19:34:52: %1-5-TRAPMGR: [396792620] traputil.c(755) 109 %% Link Down: VLAN- 1
Apr 28 19:34:52: %1-6-CLI_WEB: [1212183788] sysapi.c(2844) 106 %% Configuration file <startup-
config> read from flash!
Apr 28 19:34:51: %1-5-IP: [396819460] openr_policy.c(1438) 99 %% Added RPPI routing policy
client ospf:0.
Apr 28 19:34:51: %1-6-CLI_WEB: [1212183788] cli_txtcfg.c(542) 98 %% Configuration applied from
file <startup-config>
Apr 28 19:34:51: %1-6-CLI_WEB: [1212183788] sysapi.c(2844) 97 %% Configuration file <startup-
config> read from flash!
Apr 28 19:34:50: %1-6-General: [1209039980] procmgr.c(800) 94 %% Application Started (opensshd,
ID = 8, PID = 936
Apr 28 19:34:50: %1-5-General: [1209039980] procmgr.c(2436) 93 %% Administrative Command:app-
start opensshd
Apr 28 11:34:49: %1-6-DOT3AD: [396784740] dot3ad_cnfgr.c(1192) 20 %% Tech Support Registration
failed for DOT3AD related commands
Apr 28 11:34:45: %1-6-General: [1209039980] procmgr.c(800) 19 %% Application Started
(traceroute-0, ID = 12, PID = 916
Apr 28 11:34:45: %1-5-General: [1209039980] procmgr.c(2436) 18 %% Administrative Command:app-
start traceroute-0
Apr 28 11:34:45: %1-6-General: [1209039980] procmgr.c(800) 17 %% Application Started (ping-0, ID
= 11, PID = 909
Apr 28 11:34:45: %1-5-General: [1209039980] procmgr.c(2436) 16 %% Administrative Command:app-
start ping-0
Apr 28 11:34:44: %1-5-OSAPI: [1289614252] osapi_monitor.c(145) 15 %% Watchdog timer is started.
```

```
Apr 28 11:34:44: %1-6-General: [1209039980] procmgr.c(800) 14 %% Application Started (ospf-00,
ID = 10, PID = 851
Apr 28 11:34:44: %1-5-General: [1209039980] procmgr.c(2436) 13 %% Administrative Command:app-
start ospf-00 0
Apr 28 11:34:44: %1-6-General: [1209039980] procmgr.c(800) 12 %% Application Started (vr-agent-
0, ID = 9, PID = 845
Apr 28 11:34:44: %1-5-General: [1209039980] procmgr.c(2436) 10 %% Administrative Command:app-
start vr-agent-0
Apr 28 11:34:44: %1-6-VR_AGENT: [1289691836] vr_agent_api.c(73) 7 %% initialized the clnt
addr:/tmp/fpcvragent.00,family:1
Apr 28 11:34:43: %1-1-SIM: [1289691836] sim_util.c(3877) 5 %% Switch was reset due to operator
intervention.
Apr 28 11:34:43: %1-5-BSP: [396148460] bootos.c(178) 4 %% BSP initialization complete, starting
switch firmware.
Apr 28 11:34:35: %1-5-General: [396148460] sdm_template_mgr.c(494) 3 %% Booting with default SDM
template Data Center - IPv4 and IPv6.
Apr 28 11:34:34: %1-6-General: [1209039980] procmgr.c(3677) 2 %% Application Terminated
(user.start, ID = 7, PID = 686
Apr 28 11:34:33: %1-1-General: [396148460] usmdb_sim.c(3921) 1 %% Reboot 1 (0x1)

(Pakedge-MS-1212-189667) #
```

3.6.3. Logging buffered

This command is used to enable or disable logging to in-memory log.

Format [no] logging buffered

Default Enabled

Mode Global Config

3.6.4. Logging buffered severity level

This command sets logging severity level. The logging buffered only records the messages which of level is equal or above severity level.

The parameters “severitylevel” could be specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Format logging buffered [<severitylevel keyword> | <0 ~ 7>]

Default Info

Mode Global Config

Example: Below two examples are some configurations, it sets severity level of logging buffered to warning.

```
(Pakedge-MS-1212-189667) #logging buffered 4

(Pakedge-MS-1212-189667) #logging buffered warning
```

3.6.5. Logging buffered wrap

This command enables wrapping of in-memory logging, it will overwrite old log records when full capacity reached. Otherwise when full capacity is reached, logging stops.

Format [no] logging buffered wrap

Default Enabled

Mode Global Config

3.6.6. Clear logging buffered

This command clears all in-memory logs.

Format clear logging buffered

Default None

Mode Privilege EXEC

3.6.7. Show logging traplogs

This command displays the trap log maintained by the switch. Trap log is not retained across a switch reset.

Format show logging traplogs

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show logging traplogs
```

```
Number of Traps Since Last Reset..... 5

Trap Log Capacity..... 256

Number of Traps Since Log Last Viewed..... 5


Log System Up Time           Trap

--- ------------------------ ----------------------------------------------

  0 Apr 28 19:35:51 2000     Cold Start: Unit: 0

  1 Apr 28 19:35:05 2000     Temperature state change alarm: Unit Number: 1

                             Current: Normal, Previous: None

  2 Apr 28 19:34:59 2000     Succeeded User Login: Console started for user

                             admin connected from EIA-232.

  3 Apr 28 19:34:57 2000     Entity Database: Configuration Changed

  4 Apr 28 19:34:52 2000     Link Down: VLAN- 1


(Pakedge-MS-1212-189667) #
```

3.6.8. Show logging hosts

This command displays the configuration of logging hosts.

Format show logging hosts

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show logging hosts


Index   IP Address/Hostname      Type        Severity    Port     Status

-----  ------------------------ ----------  ----------  ------ -------------
```

```
1       10.1.1.100                  ipv4        critical    514     Active

2       logging-server.test.dep     dns         critical    514     Active


(Pakedge-MS-1212-189667) #
```

3.6.9. Logging host

This command is used to add addresses of remote log hosts.

The parameter “<hostaddress|hostname>” could be IPv4 address, or IPv6 address, or domain name. This parameter needs to match next parameter {dns | ipv4 | ipv6} to clarify its format.

The parameter “<port>” means the service port number of remote log host.

The parameters “severitylevel” could be specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Format logging host <hostaddress|hostname> {{dns | ipv4 | ipv6} [<port>] [<severitylevel>]}

Default <port> is 514

<severitylevel> is critical

Mode Global Config

Example: Adds two logging hosts: first one uses the format of IPv4 address, default port and, default severity level; second one uses the format of domain name, assigns server port to 514 and severity level to critical (2).

```
(Pakedge-MS-1212-189667) #configure

(Pakedge-MS-1212-189667) (Config)#logging host 10.1.1.100 ipv4

(Pakedge-MS-1212-189667) (Config)#logging host logging-server.test.dep dns 514 2
```

3.6.10. Logging host remove

This command is used to remove a remote log host.

The parameter “<hostindex>” means logging host Index which could be found in the output of “show logging hosts".

Format logging host remove <hostindex>

Default None

Mode Global Config

Example: Remove an existing log host which of index is 1.

```
(Pakedge-MS-1212-189667) #configure

(Pakedge-MS-1212-189667) (Config)#logging host remove 1
```

3.6.11. Logging host reconfigure

This command is used to reconfigure the setting of existing log host.

The parameter “<hostindex>” means logging host Index which could be found in the output of “show logging hosts".

The parameter “<hostaddress|hostname>” could be IPv4 address, or IPv6 address, or domain name.

The parameter “<port>” means the service port number of remote log host.

The parameters “severitylevel” could be specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Format logging host reconfigure <hostindex> {<hostaddress|hostname> | port <port> | severitylevel <severitylevel>}

Default None

Mode Global Config

Example: Changes the address of index 1 logging host to IPv4 address 2.2.2.2.

```
(Pakedge-MS-1212-189667) #configure

(Pakedge-MS-1212-189667) (Config)# logging host reconfigure 1 2.2.2.2
```

3.6.12. Logging syslog

This command enables or disables syslog logging.

Format [no] logging syslog

Default Disabled

Mode Global Config

3.6.13. Logging syslog port

This command sets the local port number of the log client for logging messages.

Format [no] logging syslog port <portid>

Default 514

Mode Global Config

3.6.14. Logging syslog facility

This command sets the default facility used in syslog messages for components that do not have an internally assigned facility.

The parameter "<facility>" can be one of the following keywords: kernel, user, mail, system, security, syslog, lpr, nntp, uucp, cron, auth, ftp, ntp, audit, alert, clock, local0, local1, local2, local3, local4, local5, local6, local7, all.

Format logging syslog facility <facility>

Default user

Mode Global Config

3.6.15. Logging syslog source-interface

This command is used to specify the physical or logical interface to use as the Syslog client source interface. If configured, the address of source interface is used for all Syslog communications between the Syslog server and the Syslog client. Otherwise there is no change in behavior. If the configured interface is down, the Syslog client falls back to normal behavior.

Format logging syslog source-interface {<slot/port> | network| vlan <vlan-id>}

no logging syslog source-interface

Default not configure

Mode Global Config

3.6.16. Logging console

This command enables or disables to print log message to console.

Format [no] logging console

Default Enabled

Mode Global Config

3.6.17. Logging console severity level

This command sets the severity level of logging console. The logging console only prints the messages which of level is equal or above severity level.

The parameters “severitylevel” could be specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Format logging console [<severitylevel keyword> | <0 ~ 7>]

Default Info

Mode Global Config

Example: Below two examples are some configurations, it sets severity level of logging console to warning.

```
(Pakedge-MS-1212-189667) #logging console 4

(Pakedge-MS-1212-189667) #logging console warning
```

3.6.18. Terminal length

This command sets the number of lines to be paginated and displayed on a screen for the current session.

Format terminal length <10-100>

no logging length

Default 24 lines per page

Mode Privileged EXEC

3.6.19. Logging cli-command

This command is used to enable or disable system logs the cli-command history to a file in global configuration mode.

NOS supports up to 5000 entries in cli-command history log. If the logs are more than 5000 entries, NOS removes the oldest log and writes the new entry. All the entries have the time stamp for reference.

Format [no] logging cli-command

Default Enabled

Mode Global Config

3.7. Script Management Commands

3.7.1. Script apply

This command applies the commands in the script to the switch.

Format script apply <scriptname>

Default None

Mode Privilege EXEC

3.7.2. Script delete

This command deletes a specified script or all scripts on the switch.

Format script delete {<scriptname> | all}

Default None

Mode Privilege EXEC

3.7.3. Script list

This command lists all scripts on the switch as well as the remaining available space.

Format script list

Default None

Mode Privilege EXEC

Example:

```
(Pakedge-MS-1212-189667) #script list

Configuration Script Name        Size(Bytes)
-------------------------------- -----------
```

```
1.scr                                    1092

t.scr                                    1092


2 configuration script(s) found.

5117 Kbytes free.

(Pakedge-MS-1212-189667) #
```

3.7.4. Script show

This command displays the content of a script file.

Format script show <scriptname>

Default None

Mode Privilege EXEC

Example:

```
(Pakedge-MS-1212-189667) #script show test.scr


1 : !Current Configuration:

2 : !

3 : !System Description "LY8, Runtime Code 5.4.01.12, Linux 3.8.13-rt9, U-Boot 2010.12 (Oct 03
2014 - 14:38:07) - ONIE 2014.05.03-7"

4 : !System Software Version "5.4.01.12"

5 : !System Up Time          "0 days 1 hrs 42 mins 9 secs"

6 : !Cut-through mode is configured as disabled

7 : !Additional Packages     BGP-4,QOS,Multicast,IPv6,Routing,Data Center

8 : !Current SNTP Synchronized Time: SNTP Client Mode Is Disabled

9 : !
```

```
10 : configure

11 : interface vlan 1

12 : exit

13 : vlan database

14 : exit

15 : sntp clock timezone "Taipei" 8 0 before-utc

16 : time-range

17 : line console

18 : exit

19 : line vty

20 : exit

21 : line ssh

22 : exit

23 : !

24 : interface control-plane

25 : exit

26 : router ospf

27 : exit

28 : ipv6 router ospf

29 : exit

30 : exit


(Pakedge-MS-1212-189667) #
```

3.7.5. Script validate

This command validates an assigned script by parsing each line. The validate option is intended to be used as a tool for script development.

Format script validate <scriptname>

Default None

Mode Privilege EXEC

Example:

```
(Pakedge-MS-1212-189667) #script validate test.scr


configure

vlan database

exit

sntp clock timezone "Taipei" 8 0 before-utc

time-range

interface vlan 1

exit

line console

exit

line vty

exit

line ssh

exit

interface control-plane

exit

router ospf

exit

ipv6 router ospf

exit

exit
```

```
Configuration script 'test.scr' validated.

(Pakedge-MS-1212-189667) #
```

3.8. User Account Management Commands

3.8.1. Show users

This command displays the configured user names and their settings.

Format show users

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
User Name	The name the user will use to login using the serial port, Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 64 characters, and is case sensitive. Two users are included as the factory default, admin, and guest.
User Access Mode	Shows whether the operator is able to change parameters on the switch (Privilege-15) or is only able to view them (Privilege-1). As a factory default, admin has Privilege-15 access and guest has Privilege-1 access. There can only be one Privilege-15 user and up to five Privilege-1 users.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show users

User

User Name Access Mode

---------- ----------

admin Privilege-15

guest Privilege-1

3.8.2. Show users accounts

The user can go to the CLI Privilege Exec to get all of user information, use the show users accounts Privilege command.

Format show users accounts [detail]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
User Name	The local user account's user name.
Privilege	The user's privilege level. The range of privilege level is 1 and 15. Access mode for privilege level 15 is read/write, the others is read-only.
Password Aging	Indicates number of days, since the password was configured, until the password expires.
Password Expiration Date	The current password expiration date in date format.
Lockout	Indicates whether the user account is locked out (true or false).
Roles	Indicates RBAC roles which belong to this user. This field is present, only if RBAC function is enabled.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show users accounts

UserName	Privilege	Password Aging	Password Expiry date	Lockout
admin	15	---	---	False
guest	1	---	---	False

(Pakedge-MS-1212-189667) (Config)#show users accounts detail

UserName..... admin

Privilege..... 15

Password Aging..... ---

Password Expiry..... ---

Lockout..... False

Override Complexity Check..... Disable

Password Strength..... ---

Roles..... network-admin

UserName..... guest

Privilege..... 1

Password Aging..... ---

Password Expiry..... ---

Lockout..... False

Override Complexity Check..... Disable

Password Strength..... ---

Roles..... network-operator

3.8.3. Show passwords configuration

Use this command to display the configured password management settings.

Format show passwords configuration

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Minimum Password Length	Minimum number of characters required when changing passwords.
Password Aging	Length in days that a password is valid.
Password History	Number of passwords to store for reuse prevention.

Lockout Attempts	Number of failed password login attempts before lockout.
Password Strength Check	The user to configure passwords that comply with the strong password configuration.
Minimum Password Uppercase Letters	Minimum number of uppercase characters required when changing passwords.
Minimum Password Lowercase Letters	Minimum number of lowercase characters required when changing passwords.
Minimum Password Numeric Characters	Minimum number of numeric characters required when changing passwords.
Minimum Password Special Characters	Minimum number of special characters required when changing passwords.
Maximum Password Repeated Characters	Maximum number of characters cannot repeated when changing passwords.
Maximum Password Consecutive Characters	Maximum number of characters cannot consecutive when changing passwords.
Minimum Password Character Classes	Valid range for user passwords.
Password Exclude Keywords	The password to be configured should not contain the keyword mentioned in this field.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show passwords configuration

Passwords Configuration

Minimum Password Length..... 0

Password Aging (days)..... 0

Password History..... 0

Lockout Attempts..... 0

Password Strength Check..... Disable

Minimum Password Uppercase Letters..... 2

Minimum Password Lowercase Letters..... 2

Minimum Password Numeric Characters..... 2

Minimum Password Special Characters..... 2

Maximum Password Repeated Characters..... 0

Maximum Password Consecutive Characters..... 0

Minimum Password Character Classes..... 4

Password Exclude Keywords..... <none>

3.8.4. Show passwords result

Use this command to display the last password set result information.

Format show passwords result

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Last User Whose Password Is Set	The local user account's user name.
Password Strength Check	The user's privilege level. The range of privilege level is 1 and 15. Access mode for privilege level 15 is read/write, the others is read-only.
Last Password Set Result	Indicates number of days, since the password was configured, until the password expires.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show passwords result

Last User whose password is set ..... guest

Password strength check ..... Disable

Last Password Set Result:

==========

Password Successfully Configured for User 'hello'.

3.8.5. Username

This command adds a new user (account) if space permits. The default privilege level is 1. The account <username> can be up to 64 characters in length. The name may be comprised of alphanumeric characters as well as the dash ('-') and underscore ('_'). The <username> is case-sensitive. Six user names can be defined.

This command changes the password of an existing operator. User password should not be more than 64 characters in length. If a user is authorized for authentication or encryption is enabled, the password must be 64 alphanumeric characters in length. The username and password are case-sensitive. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

Note: The admin user account cannot be deleted. The special characters allowed in the password include # $ % & ' ( ) * + , - / ; < = > @ [\ ] ^ _ ` { | } ~

Format username <username> { level <level> | nopasswd | passwd <0|7> <password>}

Parameter	Definition
<username>	A new user name (Range: up to 64 characters).
<0|7>	0 means the password is plain-text. 7 means the password is encrypted. When 7 is used, the password must be exactly 128 hexadeciaml characters in length. Maximum plain-text password length is 64 characters.
nopassword	This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.
<level>	The user level. Level 0 can be assigned by a level 15 user to another user to suspend that user's access. Range 0-15. Enter access level 1 for Read Access or 15 for Read/Write Access. If not specified where it is optional, the privilege level is 1.

Default None

Mode Global Config

no username

This command removes a user name created before.

Format no username <username>

Mode Global Config

3.8.6. Username <username> unlock

The user can go to the CLI Global Configuration Mode to unlock a locked user account, use the username <name> unlock global configuration command.

Format username <username> unlock

Parameter	Definition
<username>	A username.

Default None

Mode Global Config

3.8.7. Passwords aging

If the passwords aging is set, the local user will be prompted to change it before logging in again when the local user's password expires.

Format passwords aging <1-365>

Parameter	Definition
<1-365>	Number of days until password expires.

Default 0, no aging

Mode Global Config

no passwords aging

Use the no passwords aging return to default value 0.

Format no passwords aging

Mode Global Config

3.8.8. Passwords lock-out

Use this command to strengthen the security of the switch by locking user accounts that have failed login due to wrong passwords. When a lockout count is configured, a user that is logged in must enter the correct password within that count. Otherwise the user will be locked out from further switch access. Only a user with read/write access can re-activate a locked user account. The user can go to the CLI Global Configuration Mode to set the password lock-out count.

Format passwords lock-out <1-5>

Parameter	Definition
<1-5>	The number of password failures before account lock.

Default 0

Mode Global Config

no passwords lock-out

Use the no passwords lock-out to return to default value 0.

Format no passwords lock-out

Mode Global Config

3.8.9. Passwords min-length

The user can go to the CLI Global Configuration Mode to set the minimum password length.

Format passwords min-length <0-64>

Parameter	Definition
<0-64>	The length of password.

Default 0

Mode Global Config

no passwords min-length

Use the no passwords min-length return to default value 0.

Format no passwords min-length

Mode Global Config

3.8.10. Passwords strength-check

The user can go to the CLI Global Configuration Mode to set the password strength policy enforcement, use the passwords strength-check Global configuration command.

Format passwords strength-check

Default Disable

Mode Global Config

no passwords strength-check

Use the no passwords strength-check return to default disable.

Format no passwords strength-check

Mode Global Config

3.8.11. Passwords strength maximum

The user can go to the CLI Global Configuration Mode to set the password strength.

Format passwords strength maximum {consecutive-characters | repeated-characters} [<0-15>]

Default 0

Mode Global Config

no passwords strength maximum

Use the no passwords strength maximum {consecutive-characters | repeated-characters} return to default value 0.

Format no passwords strength maximum {consecutive-characters | repeated-characters}

Mode Global Config

3.8.12. Passwords strength minimum

The user can go to the CLI Global Configuration Mode to set the password strength.

Format passwords strength minimum {character-classes <0-4> | lowercase-letters <0-16> | numeric-characters <0-16> | special-characters <0-16> | uppercase-letters <0-16>}

Default 2

Mode Global Config

no passwords strength minimum

Use the no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters} return to default value 2.

Format no passwords strength minimum {character-classes | lowercase-letters | numeric-characters | special-characters | uppercase-letters}

Mode Global Config

3.8.13. Passwords strength exclude-keyword

The user can go to the CLI Global Configuration Mode to set the password strength, use the passwords strength exclude-keyword <keyword> Global configuration command.

Format passwords strength exclude-keyword <keyword>

Default None

Mode Global Config

no passwords strength exclude-keyword

Use the no passwords strength exclude-keyword <keyword> return to default none.

Format no passwords strength exclude-keyword <keyword>

Mode Global Config

3.9. Port-based Network Access Control Commands

This section describes the commands you use to configure port-based network access control (IEEE 802.1X). Port-based network access control allows you to permit access to network services only to and devices that are authorized and authenticated.

3.9.1. Show authentication methods

This command displays the ordered authentication methods for all authentication login lists.

Format show authentication methods

Mode Privileged EXEC

Display Message

Parameter	Definition
Authentication Login List	The authentication login listname.
Method 1	The first method in the specified authentication login list, if any.
Method 2	The second method in the specified authentication login list, if any.
Method 3	The third method in the specified authentication login list, if any.

Example: The following example displays the authentication configuration.

(Pakedge-MS-1212-189667) #show authentication methods

Login Authentication Method Lists

---

defaultList : local

networkList : local

Enable Authentication Method Lists

---

enableList : enable none

enableNetList : enable deny

Line	Login Method List	Enable Method List
Console	defaultList	enableList
Telnet	networkList	enableList
SSH	networkList	enableList

DOT1X :

3.9.2. Show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format show dot1x [summary [<slot/port>] | detail <slot/port> | statistics <slot/port>]

Mode Privileged EXEC

Display Message

If you do not use the optional parameters slot/port or vlanid, the command displays the global dot1x mode, the VLAN Assignment mode, and the Dynamic VLAN Creation mode.

Parameter	Definition
Administrative Mode	Indicates whether authentication control on the switch is enabled or disabled.

VLAN Assignment Mode	Indicates whether assignment of an authorized port to a RADIUS-assigned VLAN is allowed (enabled) or not (disabled).
Dynamic VLAN Creation Mode	Indicates whether the switch can dynamically create a RADIUS-assigned VLAN if it does not currently exist on the switch.
Monitor Mode	Indicates whether the Dot1x Monitor mode on the switch is enabled or disabled.

If you use the optional parameter summary [<slot/port>], the dot1x configurations for the specified port or all ports are displayed.

Parameter	Definition
Interface	The interface whose configuration is displayed.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | forceauthorized | auto | mac-based | authorized | unauthorized.
Operating Control Mode	The control mode under which this port is operating. Possible values are authorized | unauthorized.
Reauthentication Enabled	Indicates whether reauthentication is enabled on this port.
Port Status	Indicates whether the port is authorized or unauthorized. Possible values are authorized | unauthorized.

Example: The following shows example CLI display output for the command show dot1x summary 0/1.

```
(Pakedge-MS-1212-189667) #show dot1x summary 0/1

                                                    Operating          Reauthentication
Interface      Control Mode     Control Mode              Enabled              Port Status
-------------  ---------------  ----------------  ----------------------  ---------------
0/1            auto             N/A                       False
N/A
```

If you use the optional parameter 'detail <slot/port>', the detailed dot1x configuration for the specified port is displayed.

Parameter	Definition
Port	The interface whose configuration is displayed.
Protocol Version	The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.
PAE Capabilities	The port access entity (PAE) functionality of this port.
Control Mode	The configured control mode for this port. Possible values are force-unauthorized | forceauthorized | auto | mac-based.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize. When MAC-based authentication is enabled on the port, this parameter is deprecated.
Quiet Period	The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range 0 and 65535.
Transmit Period	The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Guest-VLAN ID	The guest VLAN identifier configured on the interface.
Guest VLAN Period	The time in seconds for which the authenticator waits before authorizing and placing the port in the Guest VLAN, if no EAPOL packets are detected on that port.
Supplicant Timeout	The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of 1 and 65535.
Server Timeout	The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of 1 and 65535.

Parameter	Definition
Maximum Requests	The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of 1 and 10.
Configured MAB mode	The dot1x MAC Authentication Bypass configuration status.
Operational MAB mode	The dot1x MAC Authentication Bypass operational status.
VLAN ID	The VLAN assigned to the port by the radius server. This is only valid when the port control mode is not Mac-based.
VLAN Assigned Reason	The reason the VLAN identified in the VLAN-assigned field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Guest VLAN, default, and Not Assigned. When the VLAN Assigned Reason is Not Assigned, it means that the port has not been assigned to any VLAN by dot1x. This only valid when the port control mode is not MAC-based.
Reauthentication Period	The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of 1 and 65535.
Reauthentication Enabled	Indicates if reauthentication is enabled on this port. Possible values are 'True" or "False".
Key Transmission Enabled	Indicates if the key is transmitted to the supplicant for the specified port. Possible values are True or False.
Control Direction	The control direction for the specified port or ports. Possible values are both or in.
Maximum Users	The maximum number of clients that can get authenticated on the port in the MAC-based dot1x authentication mode. This value is used only when the port control mode is not MACbased.
Unauthenticated VLAN ID	Indicates the unauthenticated VLAN configured for this port. This value is valid for the port only when the port control mode is not MAC-based.
Session Timeout	Indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default, Radius-Request. If the value is Default, the session is terminated the port goes into unauthorized state. If the value is Radius-Request, then a reauthentication of the client authenticated on the port is performed. This value is valid for the port only when the port control

	mode is not MAC-based.

Example: The following shows example CLI display output for the command.

(Pakedge-MS-1212-189667) #show dot1x detail 0/1

Port..... 0/1

Protocol Version..... 1

PAE Capabilities..... Authenticator

Control Mode..... auto

Authenticator PAE State..... Initialize

Backend authentication state..... Initialize

Quiet Period (secs)..... 60

Transmit Period (secs)..... 30

Guest VLAN ID..... 0

Guest VLAN Period (secs)..... 90

Supplicant Timeout (secs)..... 30

Server Timeout (secs)..... 30

Maximum Requests..... 2

Configured MAB Mode..... Disabled

Operational MAB Mode..... Disabled

VLAN Id..... 0

VLAN Assigned Reason..... Not Assigned

Reauthentication Period (secs)..... 3600

Reauthentication Enabled..... False

Key Transmission Enabled..... False

Control Direction..... both

Maximum Users..... 48

Unauthenticated VLAN ID..... 0

Session Timeout..... 0

Session Termination Action..... Default

For each client authenticated on the port, the **show dot1x detail <slot/port>** command will display the following MAC-based dot1x parameters if the port-control mode for that specific port is MAC-based.

Parameter	Definition
Supplicant MAC-Address	The MAC-address of the supplicant.
Authenticator PAE State	Current state of the authenticator PAE state machine. Possible values are Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized.
Backend Authentication State	Current state of the backend authentication state machine. Possible values are Request, Response, Success, Fail, Timeout, Idle, and Initialize.
VLAN-Assigned	The VLAN assigned to the client by the radius server.
Logical Port	The logical port number associated with the client.

If you use the optional parameter statistics <slot/port>, the following dot1x statistics for the specified port appear.

Parameter	Definition
Port	The interface whose statistics are displayed.
PAE Capabilities	The port access entity (PAE) functionality of this port.
EAPOL Frames Received	The number of valid EAPOL frames of any type that have been received by this authenticator.
EAPOL Frames Transmitted	The number of EAPOL frames of any type that have been transmitted by this authenticator.
EAPOL Start Frames Received	The number of EAPOL start frames that have been received by this authenticator.
EAPOL Logoff Frames Received	The number of EAPOL logoff frames that have been received by this authenticator.
Last EAPOL Frame Version	The protocol version number carried in the most recently received EAPOL frame.
Last EAPOL Frame Source	The source MAC address carried in the most recently received EAPOL frame.
EAP Response/Id Frames	The number of EAP response/identity frames that have been received by

Received	this authenticator.
EAP Response Frames Received	The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.
EAP Request/Id Frames Transmitted	The number of EAP request/identity frames that have been transmitted by this authenticator.
EAP Request Frames Transmitted	The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.
Invalid EAPOL Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.
EAP Length Error Frames Received	The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

3.9.3. Show dot1x authentication-history

This command is used to display the Dot1x Authentication History Log for the specified port or all ports. Use the optional keywords to display only failure authentication events in summary or in detail

Format show dot1x authentication-history {<slot/port> | all} [failed-auth-only] [detail]

Mode Privileged EXEC

Display Message

If you use the optional parameter detail, the following information for the specified port or all ports appears.

Parameter	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
MAC-Address	The supplicant/client MAC address.
VLAN assigned	The VLAN assigned to the client/port on authentication.
VLAN assigned Reason	The type of VLAN ID assigned, which can be Guest VLAN, Unauth, Default, RADIUS Assigned, or Monitor Mode VLAN ID.
Auth Status	The authentication status.

Reason	The actual reason behind the successful or failed authentication.

If you do not use the optional parameter, the following information for the specified port or all ports appears.

Parameter	Definition
Time Stamp	The exact time at which the event occurs.
Interface	Physical Port on which the event occurs.
MAC-Address	The supplicant/client MAC address.
VLAN ID	The VLAN assigned to the client/port on authentication.
Auth Status	The authentication status.

3.9.4. Show dot1x clients

This command is used to display the Dot1x client information. This command also displays information about the number of clients that are authenticated using Monitor mode and using Dot1x

Format show dot1x clients [<slot/port>]

Mode Privileged EXEC

Display Message

Parameter	Definition
Clients Authenticated using Monitor Mode	Indicates the number of the Dot1x clients authenticated using Monitor mode.
Clients Authenticated using Dot1x	Indicates the number of Dot1x clients authenticated using 802.1x authentication process.
Logical Interface	The logical port number associated with a client.
Interface	The physical port to which the supplicant is associated.
User Name	The user name used by the client to authenticate to the server.
Supp MAC Address	The supplicant device MAC address.
Session Time	The time since the supplicant is logged on.

VLAN ID	The VLAN assigned to the port.
VLAN Assigned	The reason the VLAN identified in the VLAN ID field has been assigned to the port. Possible values are RADIUS, Unauthenticated VLAN, Monitor Mode, or Default. When the VLAN Assigned reason is Default, it means that the VLAN was assigned to the port because the P-VID of the port was that VLAN ID.
Session Timeout	This value indicates the time for which the given session is valid. The time period in seconds is returned by the RADIUS server on authentication of the port. This value is valid for the port only when the port-control mode is not MAC-based.
Session Termination Action	This value indicates the action to be taken once the session timeout expires. Possible values are Default and Radius-Request. If the value is Default, the session is terminated and client details are cleared. If the value is Radius-Request, then a reauthentication of the client is performed.

3.9.5. Show dot1x users

This command is used to display the Dot1x port security user information for logically configured users

Format show dot1x users <slot/port>

Mode Privileged EXEC

Display Message

Parameter	Definition
Users	Users configured locally to have access to the specified port.

3.9.6. AAA authentication dot1x default

Use this command to configure the authentication method for port-based access to the switch. The additional methods of authentication are used only if the previous method returns an error, not if there is an authentication failure. The possible methods are as follows:

- local. Uses the local username database for authentication.
- none. Uses no authentication.
- radius. Uses the list of all RADIUS servers for authentication.

Format aaa authentication dot1x default {ias | local | none | radius}

Mode Global Config

3.9.7. Clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format clear dot1x statistics {<slot/port> | all}

Mode Privileged EXEC

3.9.8. Clear dot1x authentication-history

This command clears the authentication history table captured during successful and unsuccessful authentication on all interface or the specified interface.

Format clear dot1x authentication-history [slot/port]

Mode Privileged EXEC

3.9.9. Clear RADIUS statistics

This command is used to clear all RADIUS statistics.

Format clear radius statistics

Mode Privileged EXEC

3.9.10. Dot1x eapolflood

Use this command to enable EAPOL flood support on the switch.

Format dot1x eapolflood

Default Disable

Mode Global Config

no dot1x eapolflood

This command disables EAPOL flooding on the switch.

Format no dot1x eapolflood

Mode Global Config

3.9.11. Dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Format dot1x dynamic-vlan enable

Default Disable

Mode Global Config

no dot1x dynamic-vlan enable

Use this command to prevent the switch from creating VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Format no dot1x dynamic-vlan enable

Mode Global Config

3.9.12. Dot1x guest-vlan

This command configures VLAN as guest vlan on an interface. The command specifies an active VLAN as an IEEE 802.1X guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Format dot1x guest-vlan <vlan-id>

Default Disable

Mode Interface Config

no dot1x guest-vlan

This command disables Guest VLAN on the interface.

Format no dot1x guest-vlan

Mode Interface Config

3.9.13. Dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format dot1x initialize <slot/port>

Mode Privileged EXEC

3.9.14. Dot1x mac-auth-bypass

This command enables dot1x MAC authentication bypass on an interface.

Format dot1x mac-auth-bypass

Default Disable

Mode Interface Config

no dot1x mac-auth-bypass

This command disables dot1x MAC authentication bypass on an interface.

Format no dot1x mac-auth-bypass

Default Disable

Mode Interface Config

3.9.15. Dot1x max-req

This command sets the maximum number of times the authenticator state machine on an interface will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format dot1x max-req <1-10>

Default 2

Mode Interface Config

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format no dot1x max-req

Mode Interface Config

3.9.16. Dot1x max-users

Use this command to set the maximum number of clients supported on an interface when MAC-based dot1x authentication is enabled on the port. The *count* value is in the range 1 - 48.

Format dot1x max-users <count>

Default 48

Mode Interface Config

no dot1x max-users

This command resets the maximum number of clients allowed per port to its default value.

Format no dot1x max-users

Mode Interface Config

3.9.17. Dot1x port-control

This command sets the authentication mode to use on the specified interface. Use the force-unauthorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Use the force-authorized parameter to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Use the auto parameter to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Format dot1x port-control {force-unauthorized | force-authorized | auto | mac-based}

Default Auto

Mode Interface Config

no dot1x port-control

This command sets the 802.1X port control mode on the specified port to the default value.

Format no dot1x port-control

Mode Interface Config

3.9.18. Dot1x port-control all

This command sets the authentication mode to use on all ports. Select force-unauthorized to specify that the authenticator PAE unconditionally sets the controlled port to unauthorized. Select force-authorized to specify that the authenticator PAE unconditionally sets the controlled port to authorized. Select auto to specify that the authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. If the mac-based option is specified, then MAC-based dot1x authentication is enabled on the port.

Format dot1x port-control all {force-unauthorized | force-authorized | auto | mac-based}

Default Auto

Mode Global Config

no dot1x port-control all

This command sets the authentication mode on all ports to the default value.

Format no dot1x port-control all

Mode Global Config

3.9.19. Dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is auto or mac-based. If the control mode is not auto or mac-based, an error will be returned.

Format dot1x re-authenticate <slot/port>

Mode Privileged EXEC

3.9.20. Dot1x re-authentication

This command enables re-authentication of the supplicant for the specified interface.

Format dot1x re-authentication

Default Disable

Mode Interface Config

no dot1x re-authentication

This command disables re-authentication of the supplicant for the specified port.

Format no dot1x re-authentication

Mode Interface Config

3.9.21. Dot1x system-auth-control

Use this command to enable the dot1x authentication support on the switch. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Format dot1x system-auth-control

Default Disable

Mode Global Config

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format no dot1x system-auth-control

Mode Global Config

3.9.22. Dot1x system-auth-control monitor

Use this command to enable the 802.1X monitor mode on the switch. The purpose of Monitor mode is to help troubleshoot port-based authentication configuration issues without disrupting network access for hosts connected to the switch. In Monitor mode, a host is granted network access to an 802.1X-enabled port even if it fails the authentication process. The results of the process are logged for diagnostic purposes.

Format dot1x system-auth-control monitor

Default Disable

Mode Global Config

no dot1x system-auth-control monitor

This command disables the 802.1X Monitor mode on the switch.

Format no dot1x system-auth-control monitor

Mode Global Config

3.9.23. Dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on an interface. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported:

Format dot1x timeout {{guest-vlan-period <seconds>} | {reauth-period <seconds>} | {quiet-period <seconds>} | {tx-period <seconds>} | {supp-timeout <seconds>} | {server-timeout <seconds>}}

Tokens	Definition
guest-vlan-period	The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
reauth-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.
quiet-period	The value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
tx-period	The value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
supp-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
server-timeout	The value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Default guest-vlan-period: 90 seconds
reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds

Mode Interface Config

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format no dot1x timeout {guest-vlan-period | reauth-period | quiet-period | tx-period | supptimeout | server-timeout}

Mode Interface Config

3.9.24. Dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface. The unauthenticated VLAN ID can be a valid VLAN ID from 0-Maximum supported VLAN ID (4093). The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Format dot1x unauthenticated-vlan <vlan-id>

Default 0

Mode Interface Config

no dot1x unauthenticated-vlan

This command resets the unauthenticated-vlan associated with the port to its default value.

Format no dot1x unauthenticated-vlan

Mode Interface Config

3.9.25. Dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The user parameter must be a configured user.

Format dot1x user <user> {<slot/port> | all}

Mode Global Config

no dot1x user

This command removes the user from the list of users with access to the specified port or all ports.

Format no dot1x user <user> {<slot/port> | all}

Mode Global Config

3.10. AAA Commands

This section describes the commands you use to add, manage, and delete system users. Software has two default users: admin and guest. The admin user can view and configure system settings, and the guest user can view settings.

Note: You cannot delete the admin user. There is only one user allowed with read/write privileges. You can configure up to five read-only users on the system.

3.10.1. Show accounting

This command displays ordered methods for accounting lists.

Format show accounting

Mode Privileged EXEC
User EXEC

Example: The following shows example CLI display output for this command.

(Pakedge-MS-1212-189667) #show accounting

Number of Accounting Notifications sent at beginning of an EXEC session: 0

Errors when sending Accounting Notifications beginning of an EXEC session: 0

Number of Accounting Notifications sent at end of an EXEC session: 0

Errors when sending Accounting Notifications at end of an EXEC session: 0

Number of Accounting Notifications sent at beginning of a command execution: 0

Errors when sending Accounting Notifications at beginning of a command execution: 0

Number of Accounting Notifications sent at end of a command execution: 0

Errors when sending Accounting Notifications at end of a command execution: 0

3.10.2. Show accounting methods

This command displays configured accounting method lists.

Format show accounting methods

Mode Privileged EXEC
User EXEC

Example: The following shows example CLI display output for this command.

(Pakedge-MS-1212-189667) #show accounting methods

AcctType MethodName MethodType Method1 Method2

---------- ---------- ---------- ---------- ----------

Exec dfltExecList none tacacs

Commands dfltCmdList none tacacs

DOT1X dfltDot1xList start-stop radius

Line EXEC Method List Command Method List

---------- ---------- ----------

Console dfltExecList dfltCmdList

Telnet dfltExecList dfltCmdList

SSH dfltExecList dfltCmdList

3.10.3. AAA authentication login

This command creates an authentication login list. The <listname> is up to 12 alphanumeric characters and is not case sensitive. Up to 5 authentication login lists can be configured on the switch.

If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The possible method values are enable, line, local, none, radius and tacacs.

To authenticate a user, the authentication methods in the user's login will be attempted in order until an authentication attempt succeeds or fails.

Note: The default login list included with the default configuration cannot be changed

Format aaa authentication login {<listname> | default | network} *method1 [method2…]*

Parameter	Definition
default	Uses the listed authentication methods that follow this argument as the default list of methods when a user logs in.
listname	Character string of up to 15 characters used to name the list of authentication methods activated when a user logs in.
method1… ***[method2…]***	At least one from the following: enable. Uses the enable password for authentication. line. Uses the line password for authentication. local. Uses the local username database for authentication. none. Uses no authentication. radius. Uses the list of all RADIUS servers for authentication. tacacs. Uses the list of all TACACS servers for authentication.

Default . defaultList. Used by the console and only contains the method none.

. networkList. Used by telnet and SSH and only contains the method local.

Mode Global Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config)#aaa authentication login default radius local enable none

no aaa authentication login

This command returns to the default.

Format no aaa authentication login {<listname> | default | network}

Mode Global Config

3.10.4. AAA accounting

Use this command in Global config mode to create an accounting method list for either user EXEC sessions or for user-executed commands. This list is identified by **default** or a user-specified **listname**. Accounting records, when enabled for a line-mode, can be sent at both the beginning and at the end (**start-stop**) or only at the end (**stop-only**). If **none** is specified, then accounting is disabled for the specified list. If **tacacs** is

specified as the accounting method, accounting records are notified to a TACACS+ server. If **radius** is the specified accounting method, accounting records are notified to a RADIUS server.

Note: Please note the following:

- A maximum of five Accounting Method lists can be created for each exec and command type.
- The same list-name can be used for both exec and commands accounting type.
- AAA Accounting for commands with RADIUS as the accounting method is not supported.
- Only the default Accounting Method list can be created for DOT1X. There is no provision to create mode.
- Start-stop or None are the only supported record types for DOT1X accounting. Start-stop enables accounting and None disables accounting.
- RADIUS is the only accounting method type supported for DOT1X accounting.

Format aaa accounting {exec | commands | dot1x} {default | <listname>} {start-stop | stop-only | none} *method1 [method2…]*

Parameter	Definition
exec	Provides accounting for a user EXEC terminal sessions.
commands	Provides accounting for all user executed commands.
dot1x	Provides accounting for DOT1X user commands.
default	The default list of methods for accounting services.
listname	Character string used to name the list of accounting methods.
start-stop	Sends a start accounting notice at the beginning of a process and a stop accounting notice at the beginning of a process and a stop accounting notice at the end of a process.
stop-only	Sends a stop accounting notice at the end of the requested user process.
none	Disables accounting services on this line.
method	Use either TACACS or the radius server for accounting purposes.

Mode Global Config

no aaa accounting

This command deletes the accounting method list.

Format no aaa accounting {exec | commands | dot1x} {default | <listname>}

Mode Global Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config)#aaa accounting commands userCmdAudit stop-only tacacs

(Pakedge-MS-1212-189667) (Config)#no aaa accounting commands userCmdAudit

3.10.5. Accounting

Use this command in Line Configuration mode to apply the accounting method list to a line config (console/telnet/ssh).

Format accounting {exec | commands} {default | <listname>}

Parameter	Definition
exec	Causes accounting for an EXEC session.
commands	This causes accounting for each command execution attempt. If a user is enabling accounting for exec mode for the current line-configuration type, the user will be logged out.
default	The default list of methods for accounting services.
listname	Enter a string of not more than 15 characters.

Mode Line Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config)#line console

(Pakedge-MS-1212-189667) (Config-line)#accounting exec default

(Pakedge-MS-1212-189667) (Config-line)#exit

no aaa accounting

Use this command to remove accounting from a Line Configuration mode.

Format no accounting {exec | commands}

Mode Line Config

3.11. RADIUS Commands

This section describes the commands you use to use a Remote Authentication Dial-In User Service (RADIUS) server on your network for authentication and accounting.

3.11.1. Show radius

This command displays the various RADIUS configuration items for the switch.

Format show radius

Mode Privileged EXEC

Display Message

Parameter	Definition
Number of Configured Authentication Servers	The number of RADIUS Authentication servers that have been configured.
Number of Configured Accounting Servers	The number of RADIUS Accounting servers that have been configured.
Number of Named Authentication Server Groups	The number of configured named RADIUS server groups.
Number of Named Accounting Server Groups	The number of configured named RADIUS server groups.
Number of Dead RADIUS Authentication Servers	The number of RADIUS authentication servers that are considered to be unresponsive based on the dead-time criteria.
Number of Dead RADIUS Accounting Servers	The number of RADIUS accounting servers that are considered to be unresponsive based on the dead-time criteria.
Dead Time	The amount of time to skip a RADIUS server that is not responding to authentication requests.
Dead Criteria Time	Number of seconds during which a RADIUS client need not get a valid response from the RADIUS server.
Dead Criteria Tries	Number of times that a RADIUS client attempts to get a valid response before the RADIUS server is considered as unavailable.
Timeout Duration	The configured timeout value, in seconds, for request retransmissions.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.

RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter that specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.
RADIUS Attribute 95 Mode	A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 95 Value	A global parameter that specifies the IPv6 address to be used in the NAS-IPv6-Address attributes to be used in RADIUS requests.
RADIUS Attribute 30 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 30.
RADIUS Attribute 31 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).
RADIUS Attribute 32 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier).
RADIUS Attribute 32 format	The format for RADIUS attribute 32, which is one or more of the following: • %m: MAC address • %i: IP address • %h: Host Name • %d: Domain Name.
RADIUS Attribute 44 include in access request	Indicates whether RADIUS attribute 44 is sent to the RADIUS server in access-request and accounting-request messages.

Example: The following shows an example of the command.

(switch) #show radius

Number of Configured Authentication Servers.... 1

Number of Configured Accounting Servers..... 1

Number of Named Authentication Server Groups... 1

Number of Named Accounting Server Groups..... 1

Number of Dead RADIUS Authentication Servers... 0

Number of Dead RADIUS Accounting Servers..... 0

Dead Time..... 0

Dead Criteria Time..... 20

Dead Criteria Tries..... 4

Timeout Duration..... 5

RADIUS Accounting Mode..... Disable

RADIUS Attribute 4 Mode..... Disable

RADIUS Attribute 4 Value..... 0.0.0.0

RADIUS Attribute 95 Mode..... Disable

RADIUS Attribute 95 Value..... ::

RADIUS Attribute 30 Mac Format..... legacy lower-case

RADIUS Attribute 31 Mac Format..... legacy lower-case

RADIUS Attribute 32 Mac Format..... legacy lower-case

RADIUS Attribute 32 include in access request.. Disable

RADIUS Attribute 32 format..... %m

RADIUS Attribute 44 include in access request.. Disable

3.11.2. Show radius accounting

This command displays the configured RADIUS accounting mode, accounting server, and the statistics for the configured accounting server.

Format show radius accounting [<ip-address | ipv6-address | hostname> | name [<servername>] | servers | statistics {<ip-address | ipv6-address | hostname> | name <servername>}]

Mode Privileged EXEC

Display Message

If the optional token '<ip-address | ipv6-address | hostname>' or ‘name <servername>’ is included.

Parameter	Definition
RADIUS Accounting Server IP Address	The IP Address, IPv6 Address, link local address of the configured RADIUS accounting server.

RADIUS Accounting Server Name	The name of the configured RADIUS accounting server.
RADIUS Accounting Mode	A global parameter to indicate whether the accounting mode for all the servers is enabled or not.
Link local interface	If configured, the interface associated with the link-local IPv6 address.
Port	The port used for communication with the accounting server.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.
Server State	The administrative state of the server.
Server Immortal State	Indicates whether the server is an immortal RADIUS server, which is a dead server that is marked as alive after being determined to be dead because it is the last server known to be alive.
Test User	The name of the configured RAIDUS server test user.
Idle Time	The number of minutes between RADIUS server test probes.

If the optional token 'statistics <ip-address | ipv6-address | hostname>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Parameter	Definition
RADIUS Accounting Server Name	The name of the configured RADIUS accounting server.
RADIUS Accounting Server Host Address	The IP Address, IPv6 Address, link local address of the configured RADIUS accounting server.
Round Trip Time	The time interval in hundredths of seconds, between the most recent Accounting- Response and the Accounting-Request that matched it from the RADIUS accounting server.
Requests	The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.
Retransmissions	The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.
Responses	The number of RADIUS packets received on the accounting port from this server.

Malformed Responses	The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.
Bad Authenticators	The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.
Pending Requests	The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.
Timeouts	The number of accounting timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the accounting port.
Packets Dropped	The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

Example: The following shows an example of the command.

(switch) #show radius accounting 10.0.0.1

RADIUS Accounting Server IP Address..... 10.0.0.1

RADIUS Accounting Server Name..... Default-RADIUS-Server

RADIUS Accounting Mode..... Disable

Link local interface..... Not Available

Port..... 1813

Secret Configured..... No

Server State..... Up

Server Immortal State..... False

Test User.....

Idle Time..... 60

(switch) #show radius accounting name

Server Name Host Address Port Secret

Configured

--- --- --- ---

Default-RADIUS-Server 10.0.0.1 1813 No

(Switch) #show radius accounting servers

* Host Address Server Name Port

--- --- --- ---

* 10.0.0.1 Default-RADIUS-Server 1813

* currently selected server

(switch) #show radius accounting statistics 10.0.0.1

RADIUS Accounting Server Host Address..... 10.0.0.1

Round Trip Time..... 0

Requests..... 0

Retransmissions..... 0

Responses..... 0

Malformed Responses..... 0

Bad Authenticators..... 0

Pending Requests..... 0

Timeouts..... 0

Unknown Types..... 0

Packets Dropped..... 0

3.11.3. Show radius servers

This command displays items of the configured RADIUS authenticating servers.

Format show radius servers [<ip-address | ipv6-address | hostname> | name <servername>]

Mode Privileged EXEC

Display Message

If you do not specify any parameters, then only the accounting mode and the RADIUS accounting server details are displayed.

Parameter	Definition
current selected server	The '*' symbol preceding the server host address specifies that the server is currently active.
Host Address	The IP address, IPv6 address or host name of the authenticating server.
Server Name	The Name of the authenticating server.
Port	The port used for communication with the accounting server.
Type	Specifies whether this server is a primary or secondary type.

If the optional token '<ip-address | ipv6-address | hostname>' or 'name <servername>' is included.

Parameter	Definition
RADIUS Server IP Address	The IP address, IPv6 address or host name of the authenticating server.
RADIUS Server Name	The Name of the authenticating server.
Dead Time	The amount of time to skip a RADIUS server that is not responding to authentication requests.
Timeout Duration	The configured timeout value, in seconds, for request re-transmissions.
Server State	The administrative state of the RADIUS server.

Server Immortal State	Indicates whether the server is an immortal RADIUS server, which is a dead server that is marked as alive after being determined to be dead because it is the last server known to be alive.
Test User	The name of the configured RAIDUS server test user.
Idle Time	The number of minutes between RADIUS server test probes.
RADIUS Accounting Mode	A global parameter to indicates whether the accounting mode for the server is enabled or not.
RADIUS Attribute 4 Mode	A global parameter to indicate whether the NAS-IP-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 4 Value	A global parameter to specifies the IP address to be used in the NAS-IP-Address attribute to be used in RADIUS requests.
RADIUS Attribute 95 Mode	A global parameter to indicate whether the NAS-IPv6-Address attribute has been enabled to use in RADIUS requests.
RADIUS Attribute 95 Value	A global parameter to specifies the IPv6 address to be used in the NAS-IPv6-Address attribute to be used in RADIUS requests.
RADIUS Attribute 30 MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 30.
RADIUS Attribute 31MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 31 (Calling-Station-ID).
RADIUS Attribute 32MAC Format	The format in which the MAC address is sent to the RADIUS server in attribute 32 (NAS-Identifier).
RADIUS Attribute 32 include in access request	Indicates whether RADIUS attribute 32 is sent to the RADIUS server in access-request and accounting-request messages.
RADIUS Attribute 32 format	The format for RADIUS attribute 32, which is one or more of the following: • %m: MAC address • %i: IP address • %h: Host Name • %d: Domain Name.

RADIUS Attribute 44 include in access request	Indicates whether RADIUS attribute 44 is sent to the RADIUS server in access-request and accounting-request messages.
Link local interface	Indicate the outgoing interface for link local address
Port	The port used for communication with the accounting server.
Type	Specifies whether this server is a primary or secondary type.
Secret Configured	Yes or No Boolean value indicating whether this server is configured with a secret.
Message Authenticator	The message authenticator attribute configured for the radius server.
CoA Bounce-Host-Port	Indicates whether RADIUS server Bounce-Port messages will be processed (Accept) or ignored.
Number of CoA Requests Received	Specifies the number of CoA Requests Received
Number of CoA ACK Responses Sent	Specifies the number of CoA ACK Responses Sent
Number of CoA NAK Responses Sent	Specifies the number of CoA NACK Responses Sent
Number of CoA Requests Ignored	Specifies the number of CoA Requests Ignored
Number of CoA Missing/Unsupported Attribute R	Specifies the number of CoA Missing/Unsupported Attribute Requests
Number of CoA Session Context Not Found Request	Specifies the number of CoA Session Context Not Found Requests
Number of CoA Invalid Attribute Value Request	Specifies the number of CoA Invalid Attribute Value Requests
Number of Administratively Prohibited Request	Specifies the number of Administratively Prohibited Requests

Example: The following shows an example of the command.

(Switch) #show radius servers

* Host Address Server Name Port Type

---- ---------- ---------- ----- ---------

*	192.168.100.1	Default-RADIUS-Server	1812	Secondary
	10.0.0.1	Default-RADIUS-Server	1812	Secondary

* currently selected server

(switch) #show radius servers name

Server Name	Host Address	Port	Secret Configured
Default-RADIUS-Server	192.168.100.1	1812	No

(switch) #show radius servers 192.168.100.1

RADIUS Server IP Address..... 192.168.100.1

RADIUS Server Name..... Default-RADIUS-Server

Dead Time..... 0

Timeout Duration..... 5

Server State..... Up

Server Immortal State..... False

Test User.....

Idle Time..... 60

RADIUS Accounting Mode..... Disable

RADIUS Attribute 4 Mode..... Disable

RADIUS Attribute 4 Value..... 0.0.0.0

RADIUS Attribute 95 Mode..... Disable

RADIUS Attribute 95 Value..... ::

RADIUS Attribute 30 Mac Format..... legacy lower-case

RADIUS Attribute 31 Mac Format..... legacy lower-case

RADIUS Attribute 32 Mac Format..... legacy lower-case

RADIUS Attribute 32 include in access request.. Disable

RADIUS Attribute 32 format..... %m

RADIUS Attribute 44 include in access request.. Disable

Link local interface..... Not Available

Port..... 1812

Type..... Secondary

Secret Configured..... No

Message Authenticator..... Enable

CoA Bounce-Host-Port..... Accept

Number of CoA Requests Received..... 0

Number of CoA ACK Responses Sent..... 0

Number of CoA NAK Responses Sent..... 0

Number of CoA Requests Ignored..... 0

Number of CoA Missing/Unsupported Attribute R.. 0

Number of CoA Session Context Not Found Reque.. 0

Number of CoA Invalid Attribute Value Request.. 0

Number of Administratively Prohibited Request.. 0

3.11.4. Show radius statistics

This command displays the statistics for RADIUS or configured server. To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format show radius statistics {<ipaddr | ipv6addr | hostname> | name <servername>}

Mode Privileged EXEC

Display Message

Parameter	Definition
RADIUS Server Name	The Name of the authenticating server.
Server Host Address	The IP address, IPv6 address or host name of the authenticating server.
Round Trip Time	The time interval, in hundredths of a second, between the most recent Access-Reply, Access - Challenge and the Access-Request that matched it from the RADIUS authentication server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.
Access Retransmissions	The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.
Access Accepts	The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.
Access Rejects	The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.
Malformed Access Responses	The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.
Bad Authenticators	The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.
Pending Requests	The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.
Timeouts	The number of authentication timeouts to this server.
Unknown Types	The number of RADIUS packets of unknown types, which were received from this server on the authentication port.
Packets Dropped	The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

Example: The following shows an example of the command.

(switch) #show radius statistics 192.168.100.1

RADIUS Server Name..... Default-RADIUS-Server

Server Host Address..... 192.168.100.1

Round Trip Time..... 0

Access Requests..... 0

Access Retransmissions..... 0

Access Accepts..... 0

Access Rejects..... 0

Access Challenges..... 0

Malformed Access Responses..... 0

Bad Authenticators..... 0

Pending Requests..... 0

Timeouts..... 0

Unknown Types..... 0

Packets Dropped..... 0

3.11.5. Show radius source-interface

This command displays the configured global source interface details used for a RADIUS client. The IP address of the selected interface is used as source IP for all communications with the server.

Format show radius source-interface

Mode Privileged EXEC

Display Message

Parameter	Definition
RADIUS Client Source Interface	The interface to use as the source interface for RADIUS client.

RADIUS Client Source IPv4 Address	The IP address of the interface configured as the RADIUS client source interface.

Example: The following shows an example of the command.

(Switch) #show radius source-interface

RADIUS Client Source Interface..... network

RADIUS Client Source IPv4 Address..... 192.168.100.1 [Up]

3.11.6. Authorization network radius

This command enables the switch to accept VLAN assignment by the radius server.

Format authorization network radius

Default Disable

Mode Global Config

no authorization network radius

This command disables the switch to accept VLAN assignment by the radius server.

Format no authorization network radius

Mode Global Config

3.11.7. Clear radius dynamic-author statistics

This command clear radius dynamic authorization counters.

Format clear radius dynamic-author statistics

Mode Privileged EXEC

Example:

(Pakedge-MS-1212-189667) #clear radius dynamic-author statistics

Are you sure you want to clear statistics? (y/n) y

Statistics cleared.

3.11.8. Radius accounting mode

This command is used to enable RADIUS accounting function.

Format radius accounting mode

Default Disable

Mode Global Config

no radius accounting mode

This command is used to set the RADIUS accounting function to the default value.

Format no radius accounting mode

Mode Global Config

3.11.9. Radius server attribute 4

This command specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests. If the specific IP address is configured while enabling this attribute, the RADIUS client uses that IP address while sending NAS-IP-Address attribute in RADIUS communication.

Format radius server attribute 4 [<ipaddr>]

Parameter	Definition
4	NAS-IP-Address attribute to be used in RADIUS requests.
ipaddr	The IP address of the server.

Default None

Mode Global Config

no radius server attribute 4

This command disables the NAS-IP-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format no radius server attribute 4

Mode Global Config

3.11.10. Radius server attribute 95

This command specifies the RADIUS client to use the NAS-IPv6 Address attribute in the RADIUS requests. If the specific IPv6 address is configured while enabling this attribute, the RADIUS client uses that IPv6 address while sending NAS-IPv6-Address attribute in RADIUS communication.

Format radius server attribute 95 [<ipv6-address>]

Parameter	Definition
95	NAS-IPv6-Address attribute to be used in RADIUS requests.
ipv6-address	The IPv6 address of the server.

Default None

Mode Global Config

no radius server attribute 95

This command disables the NAS-IPv6-Address attribute global parameter for RADIUS client. When this parameter is disabled, the RADIUS client does not send the NAS-IP-Address attribute in RADIUS requests.

Format no radius server attribute 95

Mode Global Config

3.11.11. Radius server deadtime

This command configures radius server dead time (in minutes) for all RADIUS authentication servers. The dead time is the amount of time to skip a RADIUS server that is not responding to authentication requests. The valid deadtime range is 0 to 2000 minutes.

Format radius server deadtime <minutes>

Default 0

Mode Global Config

no radius server deadtime

This command is used to set dead time to the default value.

Format no radius server deadtime

Mode Global Config

3.11.12. Radius server host

This command configures the IP address or DNS name to use for communicating with the RADIUS server of a selected server type. While configuring the IP address or DNS name for the authenticating or accounting servers, you can also configure the port number and server name. If the authenticating and accounting servers are configured without a name, the command uses the 'Default-RADIUS-Server' as the default names, respectively. The same name can be configured for more than one authenticating servers and the name should be unique for accounting servers.

If the '**auth**' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional *port* parameter is used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The *port* number range is 1 - 65535, with 1812 being the default value.

Note: To reconfigure a RADIUS authentication server to use the default UDP *port*, set the *port* parameter to 1812.

If the '**acct**' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional *port* parameter is used, the command will configure the UDP port to use to connect to the RADIUS

accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

Note: To reconfigure a RADIUS accounting server to use the default UDP *port*, set the *port* parameter to 1813.

Format radius server host auth <ip-addr| ipv6-address | hostname> [name <servername>] [port <port>] [test <username>] [deadtime <minutes>] [idle-time <1-35791>]

radius server host acct <ip-addr| ipv6-address | hostname> [name <servername>] [port <port>] [test <username>] [deadtime <minutes>] [idle-time <1-35791>]

Parameter	Definition
ip-addr | ipv6-address | hohstname	This field is an IPv4 or IPv6 address or a hostname
servername	Server name
port	Port number in the range 1-65535
username	Test username
deadtime	
idle-time	

Default None

Mode Global Config

no radius server host

The no version of this command deletes the configured server entry from the list of configured RADIUS servers. If the RADIUS authenticating server being removed is the active server in the servers that are identified by the same server name, then the RADIUS client selects another server for making RADIUS transactions. If the '**auth**' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the '**acct**' token is used, the previously configured RADIUS accounting server is removed from the configuration. The *ipaddr|hostname* parameter must match the IP address or hostname of the previously configured RADIUS authentication / accounting server.

Format no radius server host {acct | auth} <ip-addr| ipv6-address | hostname>

Mode Global Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config) #radius server host acct 192.168.37.60

(Pakedge-MS-1212-189667) (Config) #radius server host acct 192.168.37.60 port 1813

(Pakedge-MS-1212-189667) (Config) #radius server host auth 192.168.37.60 name Network1_RS port 1813

(Pakedge-MS-1212-189667) (Config) #radius server host acct 192.168.37.60 name Network2_RS

(Pakedge-MS-1212-189667) (Config) #no radius server host acct 192.168.37.60

3.11.13. Radius server host link-local

This command configures the link-local-address of the RADIUS server and the outgoing interface to be used by the RADIUS client to communicate with the RADIUS server. The outgoing interface can be any physical interface or network vlan.

Format radius server host auth link-local <link-local-address> interface {<slot/port> | network} [name <servername>] [port <port>] [usage-type <8021x|login|both>]

radius server host acct link-local <link-local-address> interface {<slot/port> | network} [name <servername>] [port <port>]

Parameter	Definition
link-local	Specify the link local address
interface	Specify the outgoing interface for link local address
servername	Server name
port	Port number in the range 1-65535
usage-type	Configure the Radius server usage type. The type could be – 802.1x, login, or both

Default None

Mode Global Config

no radius server host link-local

This command removes the configured radius server link-local-address.

Format no radius server host {acct | auth} link-local <link-local-address>

Mode Global Config

3.11.14. Radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the **'auth'** or **'acct'** token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Format radius server key {acct | auth} <ipaddr| hostname> [encrypted <password>]

Default None

Mode Global Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config) # radius server key auth 192.168.37.60

Enter secret (64 characters max):******

Re-enter secret:******

3.11.15. Radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address specified used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format radius server primary <ipaddr| hostname>

Default None

Mode Global Config

3.11.16. Radius server retransmit

This command sets the maximum number of times a request packet is re-transmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Format radius server retransmit <retries>

Default 4

Mode Global Config

no radius server retransmit

This command is used to set the maximum number of retries to the default value.

Format no radius server retransmit

Mode Global Config

3.11.17. Radius server timeout

This command configures the global parameter for the RADIUS client that specifies the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Format radius server timeout <seconds>

Default 5

Mode Global Config

no radius server timeout

This command is used to set the timeout value to the default value.

Format no radius server timeout

Mode Global Config

3.11.18. Radius source-interface

Use this command to specify the physical or logical interface to use as the RADIUS client source interface (Source IP address). If configured, the address of source Interface is used for all RADIUS communications between the RADIUS server and the RADIUS client. The selected source-interface IP address is used for filling the IP header of RADIUS management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address. If the configured interface is down, the RADIUS client falls back to its default behavior.

Format radius source-interface {<slot/port> | vlan <vlan-id>}

Parameter	Definition
slot/port	Specifies the interface to use as the source interface.
vlan-id	Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default None

Mode Global Config

no radius source-interface

Use this command to reset the RADIUS source interface to the default settings.

Format no radius source-interface

Mode Global Config

3.12. TACACS+ Commands

TACACS+ provides access control for networked devices via one or more centralized servers. Similar to RADIUS, this protocol simplifies authentication by making use of a single database that can be shared by many clients on a large network. TACACS+ is based on the TACACS protocol (described in RFC1492) but additionally provides for separate authentication, authorization, and accounting services. The original protocol was UDP based with messages passed in clear text over the network; TACACS+ uses TCP to ensure reliable delivery and a shared key configured on the client and daemon server to encrypt all messages.

3.12.1. Show tacacs

This command displays configured information and statistics of a TACACS+ server.

Format show tacacs [<ip-address | hostname>]

Mode Privileged EXEC

Display Message

Parameter	Definition
Host address	The IP address or hostname of the configured TACACS+ server.
Port	Shows the configured TACACS+ server port number.
Timeout	Shows the timeout in seconds for establishing a TCP connection.
Priority	Shows the preference order in which TACACS+ servers are contacted. If a server connection fails, the next highest priority server is contacted.
Link Local Interface	Shows the outgoing interface used by the link-local address

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config)#show tacacs

Global Timeout: 10

Host address	Port	Timeout	Priority
10.0.0.1	49	Global	0

3.12.2. Show tacacs source-interface

Use the `show tacacs source-interface` command in Global Config mode to display the configured global source interface details used for a TACACS+ client. The IP address of the selected interface is used as source IP for all communications with the server.

Format show tacacs source-interface

Mode Privileged EXEC

Display Message

Parameter	Definition
TACACS Client Source Interface	The interface to use as the source interface for TACACS client.
TACACS Client Source IPv4 Address	The IP address of the interface configured as the TACACS client source interface.

3.12.3. Tacacs-server host

Use the **tacacs-server host** command in Global Configuration mode to configure a TACACS+ server. This command enters into the TACACS+ configuration mode. The *ipaddr|hostname* parameter is the IPv4 or IPv6 address or hostname of the TACACS+ server. To specify multiple hosts, multiple **tacacs-server host** commands can be used.

Format tacacs-server host <ipAddr | hostname>

Mode Global Config

no tacacs-server host

This command deletes the specified hostname or IP address.

Format no tacacs-server host <ipAddr | hostname>

Mode Global Config

3.12.4. Tacacs-server host link-local

Use the **tacacs-server host link-local** command in Global Configuration mode to configure the link-local-address of the TACACS+ server and the outgoing interface to be used by the TACACS+ client to communicate with the TACACS+ server. The outgoing interface can be any physical interface.

Format tacacs-server host link-local <link-local-address> interface { <slot/port>}

Mode Global Config

no tacacs-server host link-local

This command removes the configured TACACS+ server link-local address.

Format no tacacs-server host link-local

Mode Global Config

3.12.5. Tacacs-server key

This command is used to configure the TACACS+ authentication and encryption key.

Note: The length of the secret key is up to 128 characters.

Format tacacs-server key [<key-string> | encrypted <key-string>]

Mode Global Config

no tacacs-server key

This command removes the TACACS+ server secret key.

Format no tacacs-server host <ipAddr | hostname>

Mode Global Config

3.12.6. Tacacs-server keystring

This command is used to set the global authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Note: The length of the secret key is up to 128 characters.

Format tacacs-server keysting

Mode Global Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) # tacacs-server keystring

Enter key:**********

Re-enter key:**********

3.12.7. Tacacs-server timeout

This command is used to configure the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1 to 30 seconds. If you do not specify a timeout value, the command sets the global timeout to the default value. TACACS+ servers that do not use the global timeout will retain their configured timeout values.

Format tacacs-server timeout [<timeout>]

Default 5

Mode Global Config

no tacacs-server timeout

This command restores the default timeout value for all TACACS+ servers.

Format no tacacs-server timeout

Mode Global Config

3.12.8. Key

This command is used to configure the TACACS+ authentication and encryption key.

Note: The length of the secret key is up to 128 characters.

Format key [<key-string> | encrypted <key-string>]

Mode TACACS server Config

3.12.9. Keystring

This command is used to set the TACACS+ server-specific authentication encryption key used for all TACACS+ communications between the TACACS+ server and the client.

Note: The length of the secret key is up to 128 characters.

Format keysting

Mode TACACS server Config

3.12.10. Port

This command is used to set the TACACS+ server-specific port number. The server *port-number* range is 0 to 65535.

Format port [<port-number>]

Default 49

Mode TACACS server Config

3.12.11. Priority

This command is used to set the TACACS+ server-specific authentication host priority. The server priority range is 0 to 65535.

Format priority [<priority>]

Default 0

Mode TACACS server Config

3.12.12. Timeout

This command is used to configure the timeout value for communication with the TACACS+ servers. The *timeout* parameter has a range of 1 to 30 seconds.

Format timeout [<timeout>]

Default 5

Mode TACACS server Config

3.12.13. Tacacs-server source-interface

Use this command in Global config mode to configure the source interface (Source IP address) for TACACS+ server configuration. The selected source-interface IP address is used for filling the IP header of management protocol packets. This allows security devices (firewalls) to identify the source packets coming from the specific switch.

If a source-interface is not specified, the primary IP address of the originating (outbound) interface is used as the source address.

Format tacacs-server source-interface {<slot/port> | vlan <vlan-id>}

Parameter	Definition
slot/port	Specifies the interface to use as the source interface.
vlan-id	Specifies the VLAN interface to use as the source interface. The range of VLAN ID is 1 to 4093.

Default None

Mode Global Config

no tacacs-server source-interface

Use this command in Global Configuration mode to remove the global source interface (Source IP selection) for all TACACS+ communications between the TACACS+ client and the server.

Format no tacacs-server source-interface

Mode Global Config

3.13. Security Commands

This section describes the commands you use to configure Port Security, which is also known as port MAC locking, allows you to secure the network by locking allowable MAC addresses on a given port. Packets with a matching source MAC address are forwarded normally, and all other packets are discards.

Note: To enable the SNMP trap specific to port security, see “snmp-server enable traps violation”.

3.13.1. Show port-security

This command displays the port-security settings for the port(s). If you do not use a parameter, the command displays the Port Security Administrative mode. Use the optional parameters to display the settings on a specific interface, port-channel, or on all interfaces.

Format show port-security [{<slot/port> | all | dynamic | static | violation | port-channel <portchannel-id>}]

Mode Privileged EXEC

User EXEC

Display Message

If you do not use the optional parameters *slot/port*, all, or port-channel <id>, then the command displays following information.

Parameter	Definition
Administrative Mode	Port Locking mode for the entire system. The field displays if you do not support any parameters.

For each interface, or for the interface you specify, the following information appears:

Parameter	Definition
Admin Mode	Port Locking mode for the interface.
Dynamic Limit	Maximum dynamically allocated MAC addresses.
Static Limit	Maximum statically allocated MAC addresses.
Violation Trap Mode	Whether violation traps are enabled.
Violation Shutdown	Whether violation shutdown mode are enabled.
Sticky Mode	Whether sticky mode are enabled.

Example: The following shows example CLI display output for the command.

(Pakedge-MS-1212-189667) #show port-security

Port Security Administration Mode: Disabled

(Pakedge-MS-1212-189667) #show port-security 0/1

Intf	Admin Mode	Dynamic Limit	Static Limit	Violation Trap Mode	Violation Shutdown	Sticky Mode
0/1	Disabled	600	20	Disabled	Disabled	Disabled

3.13.2. Show port-security dynamic

This command displays the dynamically locked MAC address for the port.

Format show port-security dynamic {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
MAC Address	MAC Address of dynamically locked MAC

3.13.3. Show port-security static

This command displays the statically locked MAC address for port.

Format show port-security static {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC
User EXEC

Display Message

Parameter	Definition
Number of static MAC addresses configured	The number of static MAC addresses configured
Statically Configured MAC Address	The statically configured MAC address.
VLAN ID	The ID of the VLAN that includes the host with the specified MAC address.
Sticky	Indicates whether the static MAC address entry is added in sticky mode.

Example: The following shows example CLI display output for the command.

(Pakedge-MS-1212-189667) #show port-security static 0/1

Number of static MAC addresses configured: 1

Statically configured MAC Address VLAN ID Sticky

---------- ------

00:00:01:01:00:00 2 No

3.13.4. Show port-security violation

This command displays the source MAC address of the last packet discarded on a locked port.

Format show port-security violation {<slot/port> | port-channel <portchannel-id>}

Mode Privileged EXEC

User EXEC

Display Message

Parameter	Definition
MAC Address	The source MAC Address of the last frame that was discarded at a locked port.

VLAN ID	The VLAN ID, if applicable, associated with the MAC address of the last frame that was discarded at a locked port.

3.13.5. Port-security

This command enables port locking at the system level (Global Config) or port level (Interface Config) on an interface, a range of interfaces.

Format port-security

Default Disabled

Mode Global Config
Interface Config

no port-security

This command disables port locking for one or a range of ports (Interface Config) or all (Global Config) ports.

Format no port-security

Mode Global Config
Interface Config

3.13.6. Port-security max-dynamic

This command sets the maximum number of dynamically locked MAC addresses allowed on a specific port.

Format port-security max-dynamic <0-600>

Default 600

Mode Interface Config

no port-security max-dynamic

This command resets the maximum number of dynamically locked MAC addresses allowed on a specific port to its default value.

Format no port-security max-dynamic

Mode Interface Config

3.13.7. Port-security max-static

This command sets the maximum of statically locked MAC addresses allowed on a specific port.

Format port-security max- static <0-20>

Default 20

Mode Interface Config

no port-security max-static

This command resets the maximum number of statically locked MAC addresses allowed on a specific port to its default value.

Format no port-security max- static

Mode Interface Config

3.13.8. Port-security mac-address

This command adds a MAC address to the list of statically locked MAC addresses

Format port-security mac-address <mac-address> <vlan-id>

Default None

Mode Interface Config

no port-security mac-address

This command removes a MAC address from the list of statically locked MAC addresses.

Format no port-security mac-address <mac-address> <vlan-id>

Mode Interface Config

3.13.9. Port-security mac-address move

This command converts dynamically locked MAC addresses to statically locked MAC addresses for an interface or a range of interfaces

Format port-security mac-address move

Default None

Mode Interface Config

3.13.10. Port-security mac-address sticky

This command enables sticky mode Port MAC Locking on a port. If accompanied by a MAC address and a VLAN id (for interface config mode only), it adds a sticky MAC address to the list of statically locked MAC addresses. These sticky addresses are converted back to dynamically locked addresses if sticky mode is disabled on the port. The Global command applies the "sticky" mode to all valid interfaces (physical and port-channel). There is no global sticky mode as such.

Sticky addresses that are dynamically learned will appear in show running-config as "**port-security mac-address sticky <mac-address> <vid>**" entries. This distinguishes them from the static entries.

Format port-security mac-address sticky [<mac-address> <vlan-id>]

Default None

Mode Global Config
Interface Config

no port-security mac-address sticky

This command removes the sticky mode. The sticky MAC address can be deleted by using the command "**no port-security mac-address <mac-address> <vlan-is>**".

Format no port-security mac-address sticky [<mac-address> <vlan-id>]

Mode Global Config

Interface Config

Example: The following shows an example of the command.

(Pakedge-MS-1212-189667) (Config)#port-security mac-address sticky

(Pakedge-MS-1212-189667) (Interface 0/1)#port-security mac-address sticky

(Pakedge-MS-1212-189667) (Interface 0/1)#port-security mac-address sticky 00:00:00:00:00:01 2

3.13.11. Port-security violation shutdown

This command configures the port violation shutdown mode. Once the violation happens, the interface will be shutdown

Format port-security violation shutdown

Default Disabled

Mode Interface Config

no port-security violation shutdown

This command restores violation mode to the default value.

Format no port-security violation shutdown

Mode Interface Config

3.14. SNTP (Simple Network Time Protocol) Commands

This section describes the commands you use to automatically configure the system time and date by using Simple Network Time Protocol (SNTP).

i The x86 platforms rely on the Linux NTP to manage the time zone and the time of day. The NTP is configured outside of NOS. NOS for x86 does not include the internal SNTP client and does not support SNTP commands and Time Zone clock commands.

3.14.1. Show sntp

This command displays the current time and configuration settings for the SNTP client, and indicates whether the local time has been properly updated.

Format show sntp

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Last Update Time	Time of last clock update.
Last Unicast Attempt Time	Time of last transmit query (in unicast mode).
Last Attempt Status	Status of the last SNTP request (in unicast mode) or unsolicited message (in broadcast mode).

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show sntp

Last Update Time: Jan 1 08:00:00 1970 Taipei(UTC+8:00)

Last Unicast Attempt Time: Jan 1 08:00:00 1970 Taipei(UTC+8:00)

Last Attempt Status: Other

3.14.2. Show sntp client

This command displays SNTP client settings.

Format show sntp client

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Client Supported Modes	Supported SNTP Modes (Broadcast, Unicast, or Multicast).
SNTP Version	The highest SNTP version the client supports.
Port	SNTP Client Port .
Client Mode	Configured SNTP Client Mode.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show sntp client

Client Supported Modes: unicast

SNTP Version: 4

Port: 123 (Not Configured)

Client Mode: disabled

3.14.3. Show sntp server

This command displays configured SNTP servers and SNTP server settings.

Format show sntp server

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Server Host Address	Host Address of configured SNTP Server .
Server Type	Address Type of Server.
Server Stratum	Claimed stratum of the server for the last received valid packet.
Server Reference Id	Reference clock identifier of the server for the last received valid packet.
Server Mode	SNTP Server mode.
Server Maximum Entries	Total number of SNTP Servers allowed.
Server Current Entries	Total number of SNTP configured.
Host Address	Host Address of configured SNTP Server.
Address Type	Address Type of configured SNTP server.
Priority	IP priority type of the configured server.
Version	SNTP Version number of the server. The protocol version used to query the server in unicast mode.
Port	Server Port Number
Last Attempt Time	Last server attempt time for the specified server.
Last Update Status	Last server attempt status for the server.
Total Unicast Requests	Number of requests to the server.
Failed Unicast Requests	Number of failed requests from server.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show sntp server

Server Host Address:

Server Type: unknown

Server Stratum: 0

Server Reference Id:

Server Mode: Reserved

Server Maximum Entries: 3

Server Current Entries: 1

SNTP Servers

Host Address: 10.1.1.1

Address Type: IPv4

Priority: 1

Version: 1

Port: 123

Last Attempt Time: Jan 1 08:00:00 1970 Taipei(UTC+8:00)

Last Update Status: Other

Total Unicast Requests: 0

Failed Unicast Requests: 0

3.14.4. Show sntp source-interface

Use this command to display the SNTP client source interface configured on the switch.

Format show sntp source-interface

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
SNTP Client source Interface	The interface ID of the physical or logical interface configured as the SNTP client source interface.
SNTP Client Source IPv4 Address	The IP address of the interface configured as the SNTP client source interface.

Example: The following shows examples of the CLI display output for the commands.

3.14.5. Sntp client mode unicast

This command will enable Simple Network Time Protocol (SNTP) client mode.

Format sntp client mode unicast

Default None

Mode Global Config

no sntp client mode

This command will disable Simple Network Time Protocol (SNTP) client mode.

Format no sntp client mode

Mode Global Config

3.14.6. Sntp client port

This command will set the SNTP client port id and polling interval in seconds.

Format sntp client port <portid>

Parameter	Definition
<portid>	SNTP client port id.

Default 123

Mode Global Config

no sntp client port

Resets the SNTP client port id.

Format no sntp client port

Mode Global Config

3.14.7. Sntp unicast client poll-interval

This command will set the poll interval for SNTP unicast clients in seconds.

Format sntp unicast client poll-interval <6-10>

Parameter	Definition
<6-10>	Polling interval. It's 2^(value) seconds where value is 6 to 10.

Default 6

Mode Global Config

no sntp unicast client poll-interval

This command will set the poll interval for SNTP unicast clients in seconds.

Format no sntp unicast client poll-interval <6-10>

Mode Global Config

3.14.8. Sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds.

Format sntp unicast client poll-timeout <poll-timeout>

Parameter	Definition
<poll-timeout>	Polling timeout in seconds. The range is 1 to 30.

Default 5

Mode Global Config

no sntp unicast client poll-timeout

This command will set the poll timeout for SNTP unicast clients in seconds.

Format no sntp unicast client poll-timeout

Mode Global Config

3.14.9. Sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients in seconds.

Format sntp unicast client poll-retry <poll-retry>

Parameter	Definition
<poll-retry>	Polling retry in seconds. The range is 0 to 10.

Default 1

Mode Global Config

no sntp unicast client poll-retry

This command will set the poll retry for SNTP unicast clients in seconds.

Format no sntp unicast client poll-retry

Mode Global Config

3.14.10. Sntp server

This command configures an SNTP server (with a maximum of three) where the server address can be an ip address or a domain name. The optional priority can be a value of 1-3, the version is a value of 1-4, and the port id is a value of 1-65535.

Format sntp server <ipaddress/ipv6address/domain-name> [<1-3> [<version> [<portid>]]]

Parameter	Definition
<ipaddress/ipv6address/domain-name>	IPv4 or IPv6 address or domain name of the SNTP server.
<1-3>	The range is 1 to 3.
<version>	The range is 1 to 4.

<portid>	The range is 1 to 65535.

Default None

Mode Global Config

no sntp server

This command deletes a server from the configured SNTP servers.

Format no sntp server <ipaddress/ipv6address/host-name> <addresstype>

Mode Global Config

3.14.11. clock timezone

This command sets the time zone for the switch's internal clock.

Format clock timezone {*hours*} [minutes *minutes*] [zone *acronym*]

Parameter	Definition
<name>	Name of the time zone, usually an acronym. (Range: 1-15 characters)
<0-12>	Number of hours before/after UTC. (Range: 0-12 hours)
<0-59>	Number of minutes before/after UTC. (Range: 0-59 minutes)
before-utc	Sets the local time zone before (east) of UTC.
after-utc	Sets the local time zone after (west) of UTC.

Default Taipei 08:00 Before UTC

Mode Global Config

3.14.12. Sntp source-interface

Use this command to specify the physical or logical interface to use as the SNTP client source interface. If configured, the address of source interface is used for all SNTP communications between the SNTP server and the SNTP client. Otherwise, there is no change in behavior. If the configured interface is down, the SNTP client falls back to its default behavior.

Format sntp source-interface {<slot/port> | network | vlan <vlan-id>}

Parameter	Definition
<slot/port>	Specifies the port to use as the source interface.
Network	Specifies the network vlan to use as the source interface.
<1-4093>	Specifies the VLAN interface to use as the source interface. The range of the VLAN ID is 1 to 4093.

Default None

Mode Global Config

no sntp source-interface

This command will reset the SNTP source interface to its default settings.

Format no sntp source-interface

Mode Global Config

3.15. LLDP (Link Layer Discovery Protocol) Commands

3.15.1. Show lldp

This command is used to display a summary of the current LLDP configuration.

Format show lldp

Default None

Mode Privileged Exec

Display Message

Term	Definition
Transmit Interval	Shows how frequently the system transmits local data LLDPDUs, in seconds.
Transmit Hold Multiplier	Shows the multiplier on the transmit interval that sets the TTL in local data LLDPDUs.
Reinit Delay	Shows the delay before re-initialization, in seconds.
Notification Interval	Shows how frequently the system sends remote data change notifications, in seconds.
Transmit Delay	Shows how frequently the system transmits local data LLDPDUs after a change is made in a TLV (type, length, or value) element in LLDP, in seconds.
Management-address Source Interface	Shows the source of the management interface

3.15.2. Show lldp interface

This command is used to display a summary of the current LLDP configuration for a specific interface or for all interfaces.

Format show lldp interface [<slot/port>]

Default None

Mode Privileged Exec

Display Message

Term	Definition

Interface	Shows the interface in a slot/port format.
Link	Shows whether the link is up or down.
Transmit	Shows whether the interface transmits LLDPDUs.
Receive	Shows whether the interface receives LLDPDUs.
Notify	Shows whether the interface sends remote data change notifications.
TLVs	Shows whether the interface sends optional TLVs in the LLDPDUs. The TLV codes can be 0 (Port Description), 1 (System Name), 2 (System Description), or 3 (System Capability).
Mgmt	Shows whether the interface transmits system management address information in the LLDPDUs.

3.15.3. Show lldp statistics

This command is used to display the current LLDP traffic and remote table statistics for a specific interface or for all interfaces.

Format show lldp statistics [<slot/port> | all]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Last Update	Shows the amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

Interface	Shows the interface in slot/port format.
Tx Total	Total number of LLDP packets transmitted on the port.
Rx Total	Total number of LLDP packets received on the port.
Discards	Total number of LLDP frames discarded on the port for any reason.
Errors	The number of invalid LLDP frames received on the port.
Ageout	Total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.
TLV Discards	Shows the number of TLVs discarded.
TLV Unknowns	Total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
TLV 802.1	Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-80-C2.
TLV 802.3	Total number of LLDP TLVs received on the port where the type value is 127 and OUI type is 00-12-0F.

3.15.4. Show lldp remote-device

This command is used to display summary information about remote devices that transmit current LLDP data to the system. You can show information about LLDP remote data received on all ports or on a specific port.

Format show lldp remote-device [<slot/port> | all | detail]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Local Interface	Identifies the interface that received the LLDPDU from the remote device.
Rem ID	Shows the ID of the remote device.

Chassis ID	The ID that is sent by a remote device as part of the LLDP message, it is usually a MAC address of the device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device

3.15.5. Show lldp remote-device detail

This command is used to display detailed information about remote devices that transmit current LLDP data to an interface on the system.

Format show lldp remote-device detail <slot/port>

Default None

Mode Privileged Exec

Display Message

Term	Definition
Local Interface	Identifies the interface that received the LLDPDU from the remote device.
Remote Identifier	An internal identifier to the switch to mark each remote device to the system.
Chassis ID Subtype	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the remote device.
Port ID Subtype	Identifies the type of port on the remote device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device.
System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.

System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
Time To Live	Shows the amount of time (in seconds) the remote device's information received in the LLDPDU should be treated as valid information.
MAC/PHY Configuration/Status	**Auto-Negotiation:** Identifies the auto-negotiation support and current status of the remote device. **PMD Auto-Negotiation:** The duplex and bit-rate capability of the port of the remote device. **Operational MAU Type:** Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.
Power Via MDI	**MDI Power Support:** The MDI power capabilities and status. **PSE Power Pair:** Indicates the way of feeding the voltage to the data cable. **Power Class:** PoE power class.
Link Aggregation	**Aggregation Status:** Indicates the link aggregation capabilities and the current aggregation status. **Aggregation Port Id:** Aggregated port identifier.
Maximum Frame Size	Shows the maximum frame size capability of the implemented MAC and PHY of the remote device.
Port VLAN Identity	Shows the PVID of the connected port of the remote device.
Protocol VLAN	**Status:** Indicates the port and protocol VLAN capability and status. **ID:** The PPVID number for the port of the remote device.
VLAN Name	Shows the name of the VLAN which the connected port is in.
Protocol Identity	Shows the particular protocols that are accessible through the port of the remote device.

3.15.6. Show lldp local-device

This command is used to display summary information about the advertised LLDP local data. This command can display summary information or detail for each interface.

Format show lldp local-device [<slot/port> |all | detail]

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Identifies the interface in a slot/port format.
Port ID	Shows the port ID associated with this interface.
Port Description	Shows the port description associated with the interface.

3.15.7. Show lldp local-device detail

This command is used to display detailed information about the LLDP data a specific interface transmits.

Format show lldp local-device detail <slot/port>

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	Identifies the interface that sends the LLDPDU.
Chassis ID Subtype	Shows the type of identification used in the Chassis ID field.
Chassis ID	Identifies the chassis of the local device
Port ID Subtype	Identifies the type of port on the local device.
Port ID	Shows the port number that transmitted the LLDPDU.
System Name	Shows the system name of the remote device.

System Description	Describes the remote system by identifying the system name and versions of hardware, operating system, and networking software supported in the device.
Port Description	Describes the port in an alpha-numeric format. The port description is configurable.
System Capabilities Supported	Indicates the primary function(s) of the device.
System Capabilities Enabled	Shows which of the supported system capabilities are enabled.
Management Address	For each interface on the remote device with an LLDP agent, lists the type of address the remote LLDP agent uses and specifies the address used to obtain information related to the device.
MAC/PHY Configuration/Status	**Auto-Negotiation:** Identifies the auto-negotiation support and current status of the remote device. **PMD Auto-Negotiation:** The duplex and bit-rate capability of the port of the remote device. **Operational MAU Type:** Displays the MAU type. The MAU performs physical layer functions, including digital data conversion from the Ethernet interfaces' collision detection and bit injection into the network.
Power Via MDI	**MDI Power Support:** The MDI power capabilities and status. **PSE Power Pair:** Indicates the way of feeding the voltage to the data cable. **Power Class:** PoE power class.
Link Aggregation	**Aggregation Status:** Indicates the link aggregation capabilities and the current aggregation status. **Aggregation Port Id:** Aggregated port identifier.
Maximum Frame Size	Shows the maximum frame size capability of the implemented MAC and PHY of the remote device.
Port VLAN Identity	Shows the PVID of the connected port of the remote device.
VLAN Name	Shows the name of the VLAN which the connected port is in.
Protocol Identity	Shows the particular protocols that are accessible through the port of the remote device.

3.15.8. Lldp notification

This command is used to enable remote data change notifications.

Format lldp notification

Default Disabled

Mode Interface Config

no lldp notification

This command is used to disable notifications**.**

Format no lldp notification

Mode Interface Config

3.15.9. Lldp notification-interval

This command is used to configure how frequently the system sends remote data change notifications. The <interval-seconds> parameter is the number of seconds to wait between sending notifications. The valid interval range is 5-3600 seconds.

Format lldp notification-interval <interval-seconds>

Default 5

Mode Global Config

no lldp notification-interval

This command is used to return the notification interval to the default value.

Format no lldp notification-interval

Mode Global Config

3.15.10. Lldp receive

This command is used to enable the LLDP receive capability.

Format lldp receive

Default Enable

Mode Interface Config

no lldp receive

This command is used to return the reception of LLDPDUs to the default value.

Format no lldp receive

Mode Interface Config

3.15.11. Lldp transmit

This command is used to enable the LLDP advertise capability.

Format lldp transmit

Default Enable

Mode Interface Config

no lldp transmit

This command is used to return the local data transmission capability to the default.

Format no lldp transmit

Mode Interface Config

3.15.12. Lldp transmit-mgmt

This command is used to include transmission of the local system management address information in the LLDPDUs.

Format lldp transmit-mgmt

Default None

Mode Interface Config

no lldp transmit-mgmt

This command is used to cancel inclusion of the management information in LLDPDUs.

Format no lldp transmit-mgmt

Mode Interface Config

3.15.13. Lldp transmit-tlv

This command is used to specify which optional type length values (TLVs) in the 802.1AB basic management set are transmitted in the LLDPDUs. Use sys-name to transmit the system name TLV. To configure the system name, please refer to “snmp-server” command. Use sys-descto transmit the system description TLV. Use sys-cap to transmit the system capabilities TLV. Use port-desc to transmit the port description TLV. To configure the port description, please refer to “description” command. Use org-spec to transmit the organization specific TLV.

Format lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

Default None

Mode Interface Config

no lldp transmit-tlv

This command is used to remove an optional TLV from the LLDPDUs. Use the command without parameters to remove all optional TLVs from the LLDPDU.

Format no lldp transmit-tlv [sys-desc] [sys-name] [sys-cap] [port-desc]

Mode Interface Config

3.15.14. Lldp timers

This command is used to set the timing parameters for local data transmission on ports enabled for LLDP. The <interval-seconds> determines the number of seconds to wait between transmitting local data LLDPDUs. The range is 5-32768 seconds. The <hold-value> is the multiplier on the transmit interval that sets the TTL in local data LLDPDUs. The multiplier range is 2-10. The <reinit-seconds> is the delay before re-initialization, and the range is 1-10 seconds.

Format lldp timers [interval <interval-seconds>] [hold <hold-value>] [reinit <reinit-seconds>]

Default Interval-seconds 30

Hold-value 4

Reinit-seconds 2

Mode Global Config

no lldp timers

This command is used to return any or all timing parameters for local data transmission on ports enabled for LLDP to the default values.

Format no lldp timers [interval] [hold] [reinit]

Mode Global Config

3.15.15. Lldp transmit-mgmt

This command is used to transmit management address in the LLDPDUs.

Format lldp transmit-mgmt **Default** Enable

Mode Interface Config

no lldp mgmt-address

Use the **no lldp mgmt-address** to reset this function to default value.

Format no lldp transmit-mgmt

Mode Interface Config

3.15.16. Lldp portid-subtype

This command is used to configure the port ID subtype field which is used to indicate how the port is being referenced in the Port ID field in LLDPDU.

Format lldp portid-subtype {| interface-name | mac-address}

Term	Definition
interface-alias	Interface alias name (configured by "*description*" CLI command)
interface-name	Interface system name
mac-address	MAC address of the physical port

Default Interface-name

Mode Interface Config

no lldp portid-subtype

Use the **no lldp mgmt-address** to reset this function to default value.

Format no lldp portid-subtype

Mode Interface Config

3.16. System Utilities

This section describes the commands you use to help troubleshoot connectivity issues and to restore various configurations to their factory defaults.

3.16.1. Clear

3.16.1.1. *Clear arp-cache*

This command is used to remove all dynamic ARP entries from the ARP cache.

Format clear arp-cache

Default None

Mode Privileged Exec

3.16.1.2. *Clear traplog*

This command clears the trap log.

Format clear traplog

Default None

Mode Privileged Exec

3.16.1.3. *Clear logging buffered*

This command is used to clear the message log maintained by the switch. The message log contains system trace information.

Format clear logging buffered

Default None

Mode Privileged Exec

3.16.1.4. *Clear config*

This command resets the configuration to the factory defaults without powering off the switch.

Format clear config

Default None

Mode Privileged Exec

3.16.1.5. *Clear pass*

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format clear pass

Default None

Mode Privileged Exec

3.16.1.6. *Clear counters*

This command clears the statistics for a specified slot/port, for all the ports, or MPLS counter, or for an interface on an assigned VLAN based or port channel ID.

The parameter “mplsd” means to clear Multiprotocol Label Switching counter, it includes global counters and per-label counters.

Format clear counters [<slot/port> | port-channel <portchannel-id> | loop-detection | vlan <vlan-id> | all]

Default None

Mode Privileged Exec

3.16.1.7. *Clear vlan*

This command resets VLAN configuration parameters to the factory defaults.

Format clear vlan

Default None

Mode Privileged Exec

3.16.1.8. *Clear igmp snooping*

This command clears IGMP snooping entries from the MFDB table.

Format clear igmp snooping

Default None

Mode Privileged Exec

3.16.1.9. *Clear dot1x authentication-history*

This command is used to clear 802.1x authentication history table.

Format clear dot1x authentication-history [<slot/port>]

Default None

Mode Privileged Exec

3.16.1.10. *Clear radius statistics*

This command is used to clear all RADIUS statistics.

Format clear radius statistics

Default None

Mode Privileged Exec

3.16.1.11. *Clear host*

This command is used to delete entries from the host name-to-address cache, and it clears the entries from the DNS cache maintained by the software.

The parameter “hostname” means to deletes the cached entry which matches assigned hostname.

Format clear host <all | hostname >

Default None

Mode Privileged Exec

3.16.1.12. *Clear lldp statistics*

This command is used to reset LLDP (Link Layer Discovery Protocol) statistics.

Format clear lldp statistics

Default None

Mode Privileged Exec

3.16.1.13. *Clear lldp remote-data*

This command is used to delete all information from the LLDP (Link Layer Discovery Protocol) remote data table, including MED-related information.

Format clear lldp remote-data

Default None

Mode Privileged Exec

3.16.1.14. *Clear ipv6 dhcp snooping statistics*

This command is used to DHCPv6 statistics for all interfaces.

Format clear ipv6 dhcp snooping statistics

Default None

Mode Privileged Exec

3.16.1.15. *Enable password*

This command changes the password which is used to confirm current user mode to be able to upgrade Privileged EXEC mode.

There're two types of password formats:

- The type "passwd 0" specifies password in plain text, and following <password> could use alphanumeric characters with maximum length is 64 characters.
- The type "passwd 7" specifies password in encrypted form, and following <password> must be hexadecimal digitals with length of 128 characters.

Format [no] enable passwd {0 | 7} <password>

Default None

Mode Privileged EXEC

Example: First Example sets the password of enable to plain text "testPassword", and second one set the password to encrypted string which is fixed 128 characters of hexadecimal digitals.

```
(Pakedge-MS-1212-189667) (Config)# enable passwd 0 testPassword

(Pakedge-MS-1212-189667) (Config)# enable passwd 7
0fdd841c8a524979e5ba47893efcf48b12a08619953e1b6e42cde0931198ca717cb5ff8b49795a3497e283990827c5ba
1ce32855ced76a505726dfb1ee222c4b
```

3.16.2. Copy

This command uploads and downloads files to and from the switch. You can also use the copy command to manage the dual images (active and backup) on the file system. Local URLs can be specified using FTP, TFTP. SFTP and SCP are available as additional transfer methods if the software package supports secure management. If FTP is used, a password is required.

3.16.2.1. *Upload files from switch*

This command uploads files from the switch. The parameter *url* can be specified using FTP, TFTP, SCP, or SFTP. If FTP is used, a password is required

Format copy <url>

Parameter	Definition
url	Uploads file using {tftp://<ipaddress|ipv6address[%scopeid]|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>| scp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>}.

Mode Privileged EXEC

Source Parameter	Definition
application <sourcefilename>	Uploads *sourcefilename* application file
backup-config	Uploads Backup Config file.
clibanner	Uploads Pre-login Banner file.
cpu-pkt-capture	Uploads CPU packets capture file
crash-log	Uploads Crashlog file
errorlog	Uploads Errorlog file.
factory-defaults	Uploads Factory Defaults file.
fastpath.cfg	Uploads Binary Config file.
freeradius-dictionary	Uploads FreeRADIUS dictionary file which defines Vendor Specific Attributes.
image {active | backup}	Uploads the Active or the Backup Operational Code.
log	Uploads Log file.
operational-log	Uploads Operational Log file.
running-config	Copies system config file.
script <sourcefilename>	Uploads *sourcefilename* Configuration Script file.
startup-config	Uploads Startup Config file.
startup-log	Uploads Startup Log file.
tech-support	Uploads Tech Support file.
traplog	Uploads Trap log file.

3.16.2.2. *Download files to switch*

This command downloads files to the switch. The parameter *url* can be specified using FTP, TFTP, SCP, or SFTP. If FTP is used, a password is required

Format copy <url> *destination*

Parameter	Definition
url	Downloads file using {tftp://<ipaddress|ipv6address[%scopeid]|hostname>/<filepath>/<filename>| ftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>| scp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename> | sftp://<user>@<ipaddr|ipv6address[%scopeid]|hostname>/<path>/<filename>}.

Mode Privileged EXEC

Destination Parameter	Definition
application <destfilename>	Downloads application file as *destfilename* filename
backup-config	Downloads Backup Config file
clibanner	Downloads Pre-login Banner file
factory-defaults	Downloads Factory Default file
image {active | backup}	Downloads the Active or the Backup Operational Code
license-key	Download License file
openflow-ssl-ca-cert	Downloads OpenFlow CA certificate file
openflow-ssl-cert	Downloads OpenFlow switch certificate file
openflow-ssl-priv-key	Downloads OpenFlow private key file
publickey-config	Downloads Public Key for Config Script validation
script <destfilename>	Downloads Configuration Script file as *destfilename* filename
sshkey-dsa	Downloads SSH DSA Key file
sshkey-rsa1	Downloads SSH RSA1 Key file
sshkey-rsa2	Downloads SSH RSA2 Key file
sshkey-user-public-key {dsa | rsa}	Downloads SSH user Public Key file for current user. It supports DSA or RSA Key file of OpenSSH key format.
sslpem-root	Download SSL root certificate file for SSL feature of RESTFul API. If both root certificate and server key existed, two keys will be merged as ssl.pem file
sslpem-server	Download SSL server key file for SSL feature of RESTFul API. If both root certificate and server key existed, two keys will be merged as ssl.pem file

startup-config [<destfilename>]	Downloads Config file as startup configuration file or as *destfilename* filename
tech-support-cmds	Downloads Tech support commands file

Example: The following shows an example of downloading and applying as users file.

```
(Pakedge-MS-1212-189667) #copy tftp://172.16.2.60/NOS-lb9e-5.4.01.11.stk image active
Mode..................................... TFTP
Set Server IP.................................. 172.16.2.60
Path..................................... ./
Filename..................................... NOS-lb9e-5.4.01.11.stk
Data Type..................................... Code
Destination Filename..... active

Management access will be blocked for the duration of the transfer
Are you sure you want to start? (y/n) y

File transfer in progress. Management access will be blocked for the duration of the transfer. please wait...
TFTP Code transfer starting...
File contents are valid. Copying file to flash...

File transfer operation completed successfully.
```

3.16.2.3. *Write running configuration file into flash*

This command saves the running configuration to NVRAM.

Format copy running-config {startup-config | factory-defaults}

Mode Privileged EXEC

3.16.2.4. *Manage the dual images*

This command manages the dual images (active and backup) on the file system. You can copy active code to backup image or copy backup to active image of the manager unit.

Format copy {active backup | backup active}

Mode Privileged EXEC

3.16.2.5. *Manage the dual configurations*

This command manages the dual configurations (startup and backup) on the file system. You can copy startup configuration file to backup or copy backup configuration file to startup.

Format copy {startup-config backup-config | backup-config startup-config}

Mode Privileged EXEC

3.16.3. Delete

This command deletes the backup image file from the permanent storage or the core dump file from the local file system.

Format delete backup

Mode Privileged EXEC

3.16.4. Erase Application

This command erases the application file from the permanent storage.

Format erase application <filename>

Mode Privileged EXEC

3.16.5. Erase config file

This command erases the startup-config or factory-defaults from the permanent storage. When the factory defaults is erased, the factory-defaults provided by device manufacture would be restored.

Format erase {startup-config | factory-defaults}

Mode Privileged EXEC

3.16.6. Dir

Use this command to list the files in the directory /mnt/fastpath in flash from the CLI.

Format dir

Mode Privileged EXEC

Example: The following shows an example of dir.

(Pakedge-MS-1212-189667) #dir

```
                2   drwx                4096 Mar 13 2000 10:24:58 .
               12   drwx                   0 Mar 11 2000 06:26:20 ..
               11   drwx               16384 Feb 13 2000 11:38:49 lost+found
               12   -rw-            62284359 Feb 13 2000 11:39:26 image1
               13   -rw-            62268250 Mar 13 2000 10:24:58 image2
               14   -rw-                 668 Feb 19 2000 05:07:47 ssh_host_dsa_key
               15   -rw-                 891 Feb 19 2000 05:07:39 ssh_host_rsa_key
               16   -rw-                 222 Feb 19 2000 05:07:39 ssh_host_rsa_key.pub
               17   -rw-                 525 Feb 19 2000 05:07:39 ssh_host_key
               18   -rw-                 330 Feb 19 2000 05:07:39 ssh_host_key.pub
               19   -rw-                 598 Feb 19 2000 05:07:47 ssh_host_dsa_key.pub
               20   -rw-                   5 Feb 13 2000 11:41:15 sshkey
            26241   drwx                4096 Feb 13 2000 11:41:21 ruby
           371681   drwx                4096 Feb 13 2000 11:41:23 bootstrap
           379761   drwx                4096 Feb 13 2000 11:41:53 usr
           121201   drwx                4096 Feb 13 2000 11:42:06 python
           428241   drwx                4096 Feb 13 2000 11:42:06 dstat
               21   -rw-                   0 Mar 11 2000 06:26:39 fluent.conf
               22   -rwx                  10 Feb 13 2000 11:42:08 user.start
           436321   drwx                4096 Feb 13 2000 11:42:08 crashlogs
               23   -rw-               16328 Mar 11 2000 06:26:40 log2.bin
               36   -rw-                   5 Mar 11 2000 06:26:23 ologNdx0.txt
               25   -rw-                   0 Mar 05 2000 12:48:11 slog2.txt
               33   -rw-                   5 Mar 09 2000 06:05:18 ologNdx1.txt
               27   -rw-                 172 Feb 13 2000 11:42:25 hpc_port_broad.cfg
           395921   drwx                4096 Mar 11 2000 08:45:59 user-apps
               28   -rw-                 413 Mar 11 2000 06:26:38
coredump_regular_config
               29   -rw-                  72 Mar 11 2000 06:26:38
coredump_regular_config.md5sum
               30   -rw-                  96 Mar 11 2000 06:26:40 snmpOprData.cfg
               31   -rw-                 156 Feb 13 2000 11:42:44 dh512.pem
               32   -rw-                 245 Feb 13 2000 11:42:44 dh1024.pem
               26   -rw-                   0 Mar 05 2000 12:48:11 olog2.txt
```

```
34   -rw-          0 Mar 09 2000 06:05:18 slog1.txt
24   -rw-          5 Mar 05 2000 12:48:11 ologNdx2.txt
35   -rw-          0 Mar 09 2000 06:05:18 olog1.txt
37   -rw-          0 Mar 11 2000 06:26:23 slog0.txt
38   -rw-          0 Mar 11 2000 06:26:23 olog0.txt
39   -rw-         64 Mar 11 2000 06:26:23 logNvmSave.bin
40   -rw-       2401 Mar 11 2000 06:24:45 fastpath.cfg
41   -rw-        678 Mar 11 2000 06:24:47 startup-config

Total Size: 3646722048
Bytes Free: 3354427392
```

3.16.7. Bootsystem

This command is used to specify the file or image used to start up the system. It will be the active image or backup image for subsequent reboots. If the specified image does not exist on the system, this command returns an error message.

Format bootsystem {active | backup}

Mode Privileged EXEC

3.16.8. Ping

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface.

3.16.8.1. *Ping*

Use this command to determine whether another computer is on the network. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends, three pings to the target station.

Format ping [] {<ip-address> | <ip6addr> | <hostname>} [][] [] [| ipv6 |]

Default The default count is 1.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode Privileged EXEC

User EXEC

Using the options described below, you can specify the number and size of Echo Requests and the interval between Echo Requests.

Parameter	Definition
vrf-name	The name of the virtual router in which to initiate the ping. If no virtual router is specified, the ping is initiated in the default router instance.
count	Use the **count** parameter to specify the number of ping packets (ICMP Echo requests) that are sent to the destination address specified by the ip-address field. The range for count is 1 to 15 requests.
interval	Use the **interval** parameter to specify the time between Echo Requests, in seconds. Range is 1 to 60 seconds.
size	Use the **size** parameter to specify the size, in bytes, of the payload of the Echo Requests sent. Range is 0 to 65507 bytes.
source	Use the source parameter to specify the source IP/IPv6 address or interface to use when sending the Echo requests packets.

3.16.8.2. *Ping ipv6*

Use this command to determine whether another computer is on the network. Ping provides a synchronous response when initiated from the CLI interface. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The
switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *ipv6-address|hostname* parameter to ping an interface by using
the global IPv6 address of the interface. Use the optional *size* keyword to specify the size of the ping packet.
You can utilize the ping or traceroute facilities over the service/network ports when using an IPv6 global address *ipv6-address|hostname*. Any IPv6 global address or gateway assignments to these interfaces will cause IPv6 routes to be installed within the IP stack such that the ping or traceroute request is routed out the service/network port properly. When referencing an IPv6 link-local address, you must also specify the network port interface by using the *network* parameter.

Format ping ipv6 <ipv6-address | hostname> | interface network]

Default The default count is 1.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode Privileged EXEC

User EXEC

3.16.8.3. *Ping ipv6 interface*

This command use to determine whether another computer is on the network. To use the command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends three pings to the target station. Use the *interface* keyword to ping an interface by using the link-local address or the global IPv6 address of the interface. You can use a network port, or physical interface as the source. Use the optional *size* keyword to specify the size of the ping packet. The *ipv6-address* is the link local IPv6 address of the device you want to query.

Format ping ipv6 interface {network]

Default The default count is 1.

The default interval is 3 seconds.

The default size is 0 bytes.

Mode Privileged EXEC

User EXEC

3.16.9. Traceroute

3.16.9.1. *Traceroute*

Use the traceroute command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. Traceroute continues to provide a synchronous response when initiated from the CLI.

Format traceroute [ipv6] <ip-address | hostname>]

Parameter	Definition
vrf-name	The name of the virtual router in which to initiate traceroute. Only hosts reachable from within the VRF instance can be tracerouted. If a source parameter is specified in conjunction with a vrf parameter, it must be a member of the VRF. The ipv6 parameter cannot be used in conjunction with the vrf parameter.
initTtl	Use **initTtl** to specify the initial time-to-live (TTL), the maximum number of router hops between the local and remote system. Range is 0 to 255.
maxTtl	Use **maxTtle** to specify the maximum TTL. Range is 1 to 255.
maxFail	Use **maxFail** to terminate the traceroute after failing to receive a response for this number of consecutive probes. Range is 0 to 255.
port	Use the optional **port** parameter to specify destination UDP port of the probe. This should be an unused port on the remote destination system. Range is 1 to 65535.

count	Use the **count** parameter to specify the number of probes per hop. The range for count is 1 to 10.
interval	Use the **interval** parameter to specify the time between probes, in seconds. If traceroute does receive a response to a probe within this interval, then it sends the next probe immediately. Range is 1 to 60 seconds.
size	Use the **size** parameter to specify the size of probe packets, in bytes. Range is 0 to 39936 bytes.
source	Use the **source** parameter to specify the source IP/IPv6 address or interface to use for the traceroute.

Default The default initTtl is 1.
The default maxTtl is 30.
The default maxFail is 5.
The default interval is 3 seconds.
The default count is 3.
The default port is 33434.
The default size is 0 bytes.

Mode Privileged EXEC

3.16.9.2. *Traceroute ipv6*

Use the traceroute command to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. The <ipv6-address|hostname> parameter must be a valid IPv6 address|hostname.

Format traceroute ipv6 <ipv6-address | hostname>]

Default The default initTtl is 1.
The default maxTtl is 30.
The default maxFail is 5.
The default interval is 3 seconds.
The default count is 3.
The default port is 33434.
The default size is 0 bytes.

Mode Privileged EXEC

3.16.10. Logging CLI command

This command enables the CLI command Logging feature. The Command Logging component enables the switch to log all Command Line Interface (CLI) commands issued on the system.

Format logging cli-command

Default None

Mode Global Config

3.16.11. clock set

This command is used to set the system clock.

Format clockset <mm/dd/yyy> <hh:mm:ss>

Parameter	Definition
<mm/dd/yyyy>	Date Time <mm/dd/yyyy> format. (Month <1-12>. Day <1-31>. Year <2000-2037>
<hh:mm:ss>	hh in 24-hour format (Range: 0 - 23), mm (Range: 0 - 59), ss (Range: 0 - 59)

Default None

Mode Global Config

3.16.12. Reload

This command resets the switch without powering it off. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. The LEDs on the switch indicate a successful reset.

If ONIE is installed, the os parameter is added to the reload command. This parameter enables the user to boot back into ONIE.

Format reload [| configuration]

Parameter	Definition
warm	When the Warm Reload feature is present, the reload command adds the warm option. This option reduces the time it takes to reboot a Linux switch, thereby reducing the traffic disruption in the network during a switch

	reboot. For a typical Linux Enterprise switch, the traffic disruption is reduced from about two minutes for a cold reboot to about 20 seconds for a warm reboot. Note: The Warm Reload starts only the application process. The Warm Reload does not restart the boot code, the Linux kernel and the root file system. Since the Warm Reload does not restart all components, some code upgrades require that customers perform a cold reboot. Note: Warm resets can only be initiated by the administrator and do not occur automatically.
configuration	Gracefully reloads the configuration. If no configuration file is specified, the startup-config file is loaded.
scriptname	The configuration file to load. The scriptname must include the extension.

Default None

Mode Privileged Exec

3.16.13. Configure

This command is used to activate global configuration mode.

Format Configure

Default None

Mode Privileged Exec

3.16.14. Disconnect

This command is used to close a telnet session.

Format disconnect {<0-65535> | all}

Parameter	Definition
<0-10>	telnet session ID.
all	all telnet sessions.

Default None

Mode Privileged Exec

3.16.15. Hostname

This command is used to set the prompt string.

Format hostname <prompt_string>

Default

Mode Global Config

3.16.16. Quit

This command is used to exit a CLI session.

Format quit

Default None

Mode Privileged Exec

3.16.17. AutoInstall commands

3.16.17.1. *Show autoinstall*

This command displays the current status of the AutoInstall process.

Format show autoinstall

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
AutoInstall Operation	Displays the autoinstall operation is started or stopped.
AutoInstall Persistent Mode	Displays the autoinstall persistently for next reboot cycle.

AutoSave Mode	Displays the auto-save of downloaded configuration.
AutoReboot Mode	Displays the auto-reboot, which is used to allow the switch to automatically reboot after successfully downloading an image.
AutoUpgrade Mode	Displays the upgrade mode, which is used to allow to download the newer image.
AutoInstall Retry Count	Retry Count The number of times the switch has attempted to contact the TFTP server during the current AutoInstall session.

3.16.18. Capture CPU packet commands

3.16.18.1. *Show capture*

Use this command to display packets captured and save to RAM, It is possible to capture and save into RAM, packets that are received or transmitted through the CPU. A maximum 128 packets can be saved into RAM per capturing session. A maximum 128 bytes per packet can be saved into the RAM. If a packet holds more than 128 bytes, only the first 128 bytes are saved; data more than 128 bytes is skipped and cannot be displayed in the CLI.

Capturing packets is stopped automatically when 128 packets are captured and have not yet been displayed during a capture session. Captured packets are not retained after a reload cycle.

Format show capture [packets]

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
<packets>	Specifies this parameter to display the captured packets on the CLI.
Operational Status	Displays capture status.
Current Capturing Type	Displays the current capturing type. Possible types are Line, File, and Remote.

Capturing Traffic Mode	Displays the capturing traffic mode. Possible modes are Rx, Tx, or Tx/Rx.
Line Wrap Mode	Displays the line wrap mode for Line capturing type. Default is disabled.
RPCAP Listening Port	Displays the pcap listening port number. Default listening port number is 2002.
RPCAP dump file size (KB)	Display the capture packet file size. Default file size is 512KB.
Capturing Interface	Display the capturing interface.

3.16.18.2. *Capture start*

Use this command to manually start capturing CPU packets for packets for trace. The packet capture operates in three modes: capture file, remote capture and capture line.

This command is not persistent across a reboot cycle.

Format capture start [{all | received | transmit}]

Parameter	Definition
<all>	Specifies all to capture packets for both transmitted and received packets.
<received>	Specifies received to capture only received packets.
<transmit>	Specifies transmit to capture only transmitted packets.

Default None

Mode Privileged Exec

3.16.18.3. *Capture stop*

Use this command to manually stop capturing CPU packets for packets for trace.

Format capture stop

Default None

Mode Privileged Exec

3.16.18.4. *Capture packet to file, remote or line*

Use this command to configure packet capture options. This command is persistent across a reboot cycle.

Format capture {file | remote | line}

Parameter	Definition
file	In the capture file mode, the captured packets are stored in a file on Flash. The maximum file size defaults to 512KB. The switch can transfer the file to a TFTP server via TFTP, FTP via CLI. The file is formatted in pcap format, is name cpu-pkt-capture.pcap, and can be examined using network analyzer tools such as Wireshark or Ethereal. Starting a file capture automatically terminates any remote capture sessions and line capturing. After the packet capture is activated, the capture proceeds until the capture file reaches its maximum size, or until the capture is stopped manually using CLI command „capture stop“.
Remote	In the remote capture mode, the captured packets are redirected in real time to an external PC running the wireshark tool for Microsoft Windows. A packet capture server runs on the switch side and sends the captured packets via a TCP connection to the Wireshark tool. The remote capture can be enabled or disable using the CLI. There should be a Windows PC with the Wireshark tool to display the captured file. When using the remote capture mode, the switch does not store any captured data locally on its file system.
line	In the capture line mode, the captured packets are saved into the RAM and can be displayed on the CLI. Starting a line capture automatically terminates any remote capture session and capturing into a file. There is a maximum 128 packets of maximum 128 bytes that can be captured and displayed in Line mode.

Default Remote

Mode Global Config

3.16.18.5. *Capture remote port*

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Format capture remote [port <port-id>]

Parameter	Definition
<port-id>	Configure the listening port for remote Wireshark tool. The range of port ID is 1024 to 49151.

Default 2002

Mode Global Config

3.16.18.6. *Capture file size*

Use this command to configure file capture options. This command is persistent across a reboot cycle.

Format capture file [size <file-size>]

Parameter	Definition
<file-size>	Configure the file size in KB. The range of file size is 2 to 512KB.

Default 512

Mode Global Config

3.16.18.7. *Capture line wrap*

This command enables wrapping of captured packets in line mode when the captured packets reaches full capacity. This command is persistent across a reboot cycle.

Format capture line [wrap]

Default Disable

Mode Global Config

no capture line wrap

This command disables wrapping of captured packets and configures capture packet to stop when the captured packet capacity is full.

Format no capture line wrap

Mode Global Config

3.16.19. CLIBanner

This command is used to set the pre-login CLI banner before displaying the login prompt.

Format set clibanner <line>

Default None

Mode Global Config

Parameter	Description
line	Banner text where “” (double quote) is a delimiting character. The banner message can be up to 2000 characters.

no set clibanner

This command unconfigures the pre-login CLI banner.

Format no set clibanner

Mode Global Config

3.16.20. In-Service Software Upgrade

The in-service software upgrade (ISSU) feature allows users to upgrade the switch software without interrupting data forwarding through the switch.

The goal of ISSU is to maintain Ethernet data connectivity with the servers attached to TOR switches while the TOR switch software is being upgraded. A software upgrade that requires a reboot or a kernel upgrade is not supported via ISSU.

During the ISSU process, management to the switch is disrupted. After the upgrade, users must log on to the switch again and re-authenticate to resume any switch management session.

The ISSU feature is available only on x86 platforms. As of the current NOS release, the following features support ISSU:

L2 FDB, RSTP, MSTP, 802.1Q, 802.3AD, ARP, Routing Interfaces, NDP Cache, BGP with GR, and VRF

Any feature not listed above is ISSU unaware. This means that the feature does not distinguish between an ISSU restart and a normal restart. A feature that is not ISSU-aware tends to initialize afresh without the knowledge of previous active instance of the same and can cause traffic disruption during initialization.

3.17. DHCP Snooping Commands

DHCP snooping is a security feature that monitors DHCP messages between a DHCP client and DHCP servers to filter harmful DHCP messages and to build a bindings database of {MAC address, IP address, VLAN ID, port} tuples that are considered authorized. You can enable DHCP snooping globally and on specific VLANs, and configure ports within the VLAN to be trusted or untrusted. DHCP servers must be reached through trusted ports.

The DHCP snooping binding table contains the MAC address, IP address, lease time, binding type, VLAN number, and interface information that corresponds to the local untrusted interfaces of a switch; it does not contain information regarding hosts interconnected with a trusted interface. An untrusted interface is an interface that is configured to receive messages from outside the network or firewall. A trusted interface is an interface that is configured to receive only messages from within the network.

DHCP snooping acts like a firewall between untrusted hosts and DHCP servers. It also gives you a way to differentiate between untrusted interfaces connected to the end-user and trusted interfaces connected to the DHCP server or another switch.

DHCP snooping enforces the following security rules:

DHCP packets from a DHCP server (DHCPOFFER, DHCPACK, DHCPNAK, DHCPRELEASEQUERY) are dropped if received on an untrusted port.

DHCPRELEASE and DHCPDECLINE messages are dropped if for a MAC address in the snooping database, but the binding's interface is other than the interface where the message was received.

On untrusted interfaces, the switch drops DHCP packets whose source MAC address does not match the client hardware address. This feature is a configurable option.

The hardware identifies all incoming DHCP packets on ports where DHCP snooping is enabled. DHCP snooping is enabled on a port if (a) DHCP snooping is enabled globally, and (b) the port is a member of a VLAN where DHCP snooping is enabled. On untrusted ports, the hardware traps all incoming DHCP packets to the CPU. On trusted ports, the hardware forwards client messages and copies server messages to the CPU so that DHCP snooping can learn the binding.

You can enable the switch to operate as a DHCP Layer 2 relay agent to relay DHCP requests from clients to a Layer 3 relay agent or server. The Circuit ID and Remote ID can be added to DHCP requests relayed from clients to a DHCP server. This information is included in DHCP Option 82, as specified in sections 3.1 and 3.2 of RFC3046.

3.17.1. Show ip dhcp snooping

This command displays the DHCP snooping global configurations and summaries of port configurations.

Format show ip dhcp snooping

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping

DHCP snooping is Enabled
DHCP snooping source MAC verification is enabled
DHCP snooping is enabled on the following VLANs:
1

 Interface    Trusted     Log Invalid Pkts
-----------  ----------   ----------------
0/1          Yes          No
0/2          No           No
0/3          No           No
0/4          No           No
0/5          No           No
0/6          No           No
0/7          No           No
0/8          No           No
0/9          No           No
0/10         No           No
0/11         No           No
0/12         No           No
0/13         No           No
0/14         No           No
0/15         No           No

(Pakedge-MS-1212-189667) #
```

3.17.2. Show ip dhcp snooping per interface

This command displays the DHCP snooping detail configurations for all interfaces or for a specific interface.

Format show ip dhcp snooping interfaces [<slot/port> | port-channel <portchannel-id>]

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping interfaces

Interface     Trust State     Rate Limit      Burst Interval
                                 (pps)          (seconds)
```

```
----------   -------------   -------------   ---------------
0/1          Yes             None            N/A
0/2          No              None            N/A
0/3          No              None            N/A
0/4          No              None            N/A
0/5          No              None            N/A
0/6          No              None            N/A
0/7          No              None            N/A
0/8          No              None            N/A
0/9          No              None            N/A
0/10         No              None            N/A
0/11         No              None            N/A
0/12         No              None            N/A
0/13         No              None            N/A
0/14         No              None            N/A
0/15         No              None            N/A
0/16         No              None            N/A
0/17         No              None            N/A
0/18         No              None            N/A
0/19         No              None            N/A

(Pakedge-MS-1212-189667) #
```

3.17.3. Show ip dhcp snooping binding

This command displays the DHCP Snooping binding entries.

The parameter “static” means to restrict the output based on static entries which are added by user manually.

The parameter “static” means to restrict the output based on dynamic entries which are added by DHCP Snooping automatically

Format show ip dhcp snooping binding [{static | dynamic}] [interface {<slot/port> | port-channel <portchannel-id>}] [vlan <vlan-id>]

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping binding

Total number of bindings:  363
Total number of Tentative bindings:  61
```

```
   MAC Address       IP Address      VLAN   Interface    Type    Lease (Secs)
-----------------  ---------------  ----  -----------  -------  ------------
44:0A:A7:8A:00:00        10.10.1.6     1         0/10  DYNAMIC         86383
44:0A:A7:8A:00:01        10.10.1.8     1         0/10  DYNAMIC         86383
44:0A:A7:8A:00:02       10.10.1.10     1         0/10  DYNAMIC         86383
44:0A:A7:8A:00:03       10.10.1.11     1         0/10  DYNAMIC         86383
44:0A:A7:8A:00:04       10.10.1.12     1         0/10  DYNAMIC         86383
44:0A:A7:8A:00:05       10.10.1.13     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:00        10.10.1.2     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:01        10.10.1.3     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:02        10.10.1.4     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:03        10.10.1.5     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:04        10.10.1.7     1         0/10  DYNAMIC         86383
44:0A:A7:8A:01:05        10.10.1.9     1         0/10  DYNAMIC         86383
44:0A:A7:8A:02:00       10.10.1.20     1         0/10  DYNAMIC         86383
44:0A:A7:8A:02:01       10.10.1.21     1         0/10  DYNAMIC         86383
44:0A:A7:8A:02:02       10.10.1.22     1         0/10  DYNAMIC         86383
44:0A:A7:8A:02:03       10.10.1.23     1         0/10  DYNAMIC         86383

 (Pakedge-MS-1212-189667) #
```

3.17.4. Show ip dhcp snooping database

This command displays the DHCP Snooping configuration related to the database persistency.

Format show ip dhcp snooping database

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping database

agent url:  local

write-delay:  300

(Pakedge-MS-1212-189667) #
```

3.17.5. Show ip dhcp snooping information all

This command displays the summaries of DHCP Option-82 configurations.

Format show ip dhcp snooping information all

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping information all

DHCP Information Option82 is  Enabled.

Interface   OPT82 Mode   TrustMode
---------  ------------  --------------
0/1        Enabled       trusted
0/2        Disabled      untrusted
0/3        Disabled      untrusted
0/4        Disabled      untrusted
0/5        Disabled      untrusted
0/6        Disabled      untrusted
0/7        Disabled      untrusted
0/8        Disabled      untrusted
0/9        Disabled      untrusted
0/10       Disabled      untrusted
0/11       Disabled      untrusted
0/12       Disabled      untrusted
0/13       Disabled      untrusted
0/14       Disabled      untrusted
0/15       Disabled      untrusted
0/16       Disabled      untrusted
0/17       Disabled      untrusted
0/18       Disabled      untrusted

(Pakedge-MS-1212-189667) #
```

3.17.6. Show ip dhcp snooping information statistics

This command displays DHCP Option-82 statistics per interface.

Format show ip dhcp snooping information stats interface {<slot/port> | all}

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping information stats interface all
```

```
Interface    UntrustedServer  UntrustedClient  TrustedServer    TrustedClient
             MsgsWithOpt82    MsgsWithOpt82    MsgsWithoutOpt82 MsgsWithoutOpt82
-----------  ---------------  ---------------  ---------------- ----------------
0/1          0                0                0                0
0/2          0                0                0                0
0/3          0                0                0                0
0/4          0                0                0                0
0/5          0                0                0                0
0/6          0                0                0                0
0/7          0                0                0                0
0/8          0                0                0                0
0/9          0                0                0                0
0/10         0                0                0                0
0/11         0                0                0                0
0/12         0                0                0                0
0/13         0                0                0                0
0/14         0                0                0                0
0/15         0                0                0                0
0/16         0                0                0                0
0/17         0                0                0                0
0/18         0                0                0                0
0/19         0                0                0                0

(Pakedge-MS-1212-189667) #
```

3.17.7. Show ip dhcp snooping information agent-option

This command displays the Option-82 configurations of DHCP Relay agent on specific VLAN.

Format show ip dhcp snooping information agent-option vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) # show ip dhcp snooping information agent-option vlan 1

DHCP Information Option82 is  Enabled.


VLAN Id   DHCP OPT82   CircuitId   RemoteId
---------  ---------  ----------  --------------------------------
1          Enabled    Enabled     testRemoteIdString

(Pakedge-MS-1212-189667) #
```

3.17.8. Show ip dhcp snooping information per vlan

This command displays the DHCP Option-82 configurations per specific VLAN.

Format show ip dhcp snooping information vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping information vlan 1

DHCP Information Option82 is  Enabled.

DHCP L2 Relay is enabled on the following VLANs:
1

(Pakedge-MS-1212-189667) #
```

3.17.9. Show ip dhcp snooping information circuit-id

This command displays the remote-id configuration of DHCP Option-82 per specific VLAN.

Format show ip dhcp snooping information circuit-id vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) # show ip dhcp snooping information circuit-id vlan 1

DHCP Information Option82 is Enabled.

DHCP Circuit-Id option is enabled on the following VLANs:
1

(Pakedge-MS-1212-189667) #
```

3.17.10. Show ip dhcp snooping information remote-id

This command displays the remote-id configuration of DHCP Option-82 per specific VLAN.

Format show ip dhcp snooping information remote-id vlan <vlan-list>

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) # show ip dhcp snooping information remote-id vlan 1

DHCP Information Option82 is Enabled.

VLAN ID    Remote Id
---------  --------------------------------
1          testRemoteIdString

(Pakedge-MS-1212-189667) #
```

3.17.11. Show ip dhcp snooping information interface

This command displays the remote-id configuration of DHCP Option-82 per interface.

Format show ip dhcp snooping information interface {<slot/port> | all}

Default None

Mode Privileged Exec

Example:

```
(Pakedge-MS-1212-189667) #show ip dhcp snooping information interface 0/1

DHCP Information Option82 is  Enabled.

Interface   OPT82 Mode   TrustMode
---------  ------------  --------------
0/1        Enabled       trusted

(Pakedge-MS-1212-189667) #
```

3.17.12. Ip dhcp snooping

This command enables or disables the DHCP Snooping globally.

Format [no] ip dhcp snooping

Default Disable

Mode Global Config

3.17.13. Ip dhcp snooping vlan

This command enables or disables the DHCP Snooping to the specific VLAN.

Format [no] ip dhcp snooping vlan <vlan-list>

Default Disable

Mode Global Config

3.17.14. Ip dhcp snooping verify mac-address

This command enables or disables the verification of the source MAC address with the client hardware address in the received DHCP message.

Format [no] ip dhcp snooping verify mac-address

Default Disable

Mode Global Config

3.17.15. Ip dhcp snooping database

This command configures the persistent location of the DHCP Snooping database. This can be local or a remote file on a given IP machine.

The parameter “local” means to set database access inside device.

The parameter “tftp://hostIP/filename” means to set database access on remote TFTP Server.

Format ip dhcp snooping database {local | <url>}

Default Local

Mode Global Config

3.17.16. Ip dhcp snooping database write-delay

This command configures the interval in seconds at which the DHCP Snooping database will be persisted, and this database stores the results of DHCP snooping bindings. Use keyword “no” to restore the default value of this command.

The parameter “<interval>” value ranges is from 15 to 86400 seconds.

Format ip dhcp snooping database write-delay <interval>

no ip dhcp snooping database write-delay

Default 300

Mode Global Config

3.17.17. Ip dhcp snooping binding

This command configures the static DHCP Snooping binding which binds a MAC address to assigned IP address on a specific VLAN ID and interface. Use keyword “no” to remove an existing entry of DHCP Snooping binding.

Format ip dhcp snooping binding <mac-address> vlan <vlan id> <ip address> interface {<slot/port> | port-channel < portchannel-id>}

no ip dhcp snooping binding <mac-address>

Default None

Mode Global Config

Example: To add a static entry of DHCP snooping binding which binds MAC address 00:11:22:33:44:55 to IP address 10.0.0.1 on vlan 1 and port interface 0/1.

```
(Pakedge-MS-1212-189667) #configure
(Pakedge-MS-1212-189667) (Config)#ip dhcp snooping binding 00:11:22:33:44:55 vlan 1 10.0.0.1
interface 0/1
(Pakedge-MS-1212-189667) (Config)#
```

3.17.18. Ip dhcp snooping information option

This command enables or disables the DHCP Snooping application to support information Option 82 in global configuration or a specific interface.

Format [no] ip dhcp snooping information option

Default Disable

Mode Global Config
Interface Config

3.17.19. Ip dhcp snooping information option circuit-id

This command enables or disables the DHCP Snooping Option 82 with sub-option circuit-id in a range of VLANs.

The format of circuit-id is LLLLVVVVXXYYZZ, and LLLL is the length from V to Z, VVVV is VLAN ID, XX is the Unit ID, YY is the function/module ID and ZZ is the Port number.

Format [no] ip dhcp snooping information option circuit-id vlan <vlan-list>

Default Disable

Mode Global Config

3.17.20. Ip dhcp snooping information option remote-id

This command enables or disables the DHCP Snooping Option 82 with sub-option remote-id in a range of VLANs. When it's enabled, all DHCP client's requests received to this device will be added remote-id sud-option with remote-id string.

The format of remote-id is LLLLXXXXX, and LLLL is the total length of all X, XXXXX is remote-id string which is set by user.

The parameter "<remoteId string>" defines remote-id string which of maximum length is 32 characters

Format [no] ip dhcp snooping information option remote-id <remoteId string> vlan <vlan-list>
no ip dhcp snooping information option remote-id vlan <vlan-list>

Default Disable

Mode Global Config

3.17.21. Ip dhcp snooping information option vlan

This command enables or disables the DHCP Snooping option 82 in a range of VLANs.

Format [no] ip dhcp snooping information option vlan <vlan-list>

Default Disable

Mode Global Config

3.17.22. Ip dhcp snooping information option trust

This command configures an interface to be trusted for Option-82 reception.

Format [no] ip dhcp snooping information option trust

Default Disable

Mode Interface Config

3.17.23. Ip dhcp snooping limit

This command controls the rate at which the DHCP Snooping messages come. If packet rate exceeds limitation over burst interval, the assigned port will shut down automatically. User could use interface command “shutdown” and then “no shutdown” to recover it. Use keyword “no” to restore the default value of this command.

The parameter “rate” means to the limitation of packet rate. Its range is from 0 to 300 packets per second.

The parameter “burst interval” means the time interval of packet burst could be over rate limitation. Its range is from 1 to 15 seconds.

Format ip dhcp snooping limit {rate <pps> [burst interval <seconds>]} | none

no ip dhcp snooping limit rate

Default “rate” is None

“burst interval” is 1 second.

Mode Interface Config

Example: While the packet rate of DHCP message received from port 0/1 exceeds 100 pps and consecutive time interval is over 10 seconds, the port 0/1 will be shutdown automatically.

```
(Pakedge-MS-1212-189667) #configure
(Pakedge-MS-1212-189667) (Config)#interface 0/1
(Pakedge-MS-1212-189667) (Interface 0/1)# ip dhcp snooping limit rate 100 burst interval 10
(Pakedge-MS-1212-189667) (Interface 0/1)#
```

3.17.24. Ip dhcp snooping log-invalid

This command controls logging the illegal DHCP messages to logging buffer.

Format [no] ip dhcp snooping log-invalid

Default Disabled

Mode Interface Config

3.17.25. Ip dhcp snooping trust

This command enables or disables a port as DHCP Snooping trust port.

Format [no] ip dhcp snooping trust

Default Disabled

Mode Interface Config

3.17.26. Ip dhcp snooping trust

This command enables or disables a port as DHCP Snooping trust port.

Format [no] ip dhcp snooping trust

Default Disabled

Mode Interface Config

3.17.27. Clear ip dhcp snooping binding

This command is used to clear all DHCP Snooping bindings on all interfaces or on a specific interface.

Format clear ip dhcp snooping binding [interface <slot/port>]

Default None

Mode Privileged EXEC

3.17.28. Clear ip dhcp snooping statistics

This command is used to clear all DHCP Snooping statistics.

Format clear ip dhcp snooping statistics

Default None

Mode Privileged EXEC

3.17.29. Clear ip dhcp snooping information statistics

This command is used to clear statistics of DHCP Snooping Option 82.

Format clear ip dhcp snooping information statistics interface [<slot/port> | all]

Default None

Mode Privileged EXEC

3.18. Dynamic ARP Inspection (DAI) Command

Dynamic ARP Inspection (DAI) is a security feature that rejects invalid and malicious ARP packets. DAI prevents a class of man-in-the-middle attacks, where an unfriendly station intercepts traffic for other stations by poisoning the ARP caches of its unsuspecting neighbors. The miscreant sends ARP requests or responses mapping another station's IP address to its own MAC address.

To prevent ARP poisoning attacks, a switch must ensure that only valid ARP requests and responses are relayed. DAI prevents these attacks by intercepting all ARP requests and responses. Each of these intercepted packets is verified for valid MAC address to IP address bindings before the local ARP cache is updated or the packet is forwarded to the appropriate destination. Invalid ARP packets are dropped.

DAI determines the validity of an ARP packet based on valid MAC address to IP address bindings stored in a trusted database. This database is built at runtime by DHCP snooping, provided this feature is enabled on VLANs and on the switch. DAI relies on DHCP snooping. DHCP snooping listens to DHCP message exchanges and builds a binding database of valid {MAC address, IP address, VLAN, and interface} tuples. In addition, in order to handle hosts that use statically configured IP addresses, DAI can also validate ARP packets against user-configured ARP ACLs.

When DAI is enabled, the switch drops ARP packets whose sender MAC address and sender IP address do not match an entry in the DHCP snooping bindings database. You can optionally configure additional ARP packet validation.

3.18.1. Show commands

3.18.1.1. *Show ip arp inspection statistics*

This command displays the statistics of the ARP packets processed by Dynamic ARP Inspection. Give the vlan-list argument and the command displays the statistics on all DAI-enabled VLANs in that list. Give the single vlan argument and the command displays the statistics on that VLAN. If no argument is included, the command lists a summary of the forwarded and dropped ARP packets.

Format show ip arp inspection statistics [vlan <vlan-list>]

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	Definition
VLAN	The VLAN ID for each displayed row.
DHCP Drops	The number of packets dropped due to DHCP snooping binding database match failure.

ACL Drops	The number of packets dropped due to ARP ACL rule match failure.
DHCP Permits	The number of packets permitted due to DHCP snooping binding database match.
ACL Permits	The number of packets permitted due to ARP ACL rule match.
Bad Src MAC	The number of packets dropped due to Source MAC validation failure.
Bad Dest MAC	The number of packets dropped due to Destination MAC validation failure.
Invalid IP	The number of packets dropped due to invalid IP checks.

3.18.1.2. *Show ip arp inspection*

This command displays the Dynamic ARP Inspection global configuration and configuration on all the VLANs. With the vlan-list argument (i.e. comma separated VLAN ranges), the command displays the global configuration and configuration on all the VLANs in the given VLAN list. The global configuration includes the source mac validation, destination mac validation and invalid IP validation information.

Format show ip arp inspection [vlan <vlan-list>]

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default None

Mode Privileged Exec

Display Message

Term	Definition
Source MAC Validation	Displays whether Source MAC Validation of ARP frame is enabled or disabled.
Destination MAC Validation	Displays whether Destination MAC Validation is enabled or disabled.
IP Address Validation	Displays whether IP Address Validation is enabled or disabled.
VLAN	The VLAN ID for each displayed row.
Configuration	Displays whether DAI is enabled or disabled on the VLAN.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

3.18.1.3. *Show ip arp inspection interfaces*

This command displays the Dynamic ARP Inspection configuration on all the DAI-enabled interfaces. An interface is said to be enabled for DAI if at least one VLAN, that the interface is a member of, is enabled for DAI. Given a interface argument, the command displays the values for that interface whether the interface is enabled for DAI or not.

Format show ip arp inspection [vlan <vlan-list>]

Term	Definition
<slot/port>	Interface Number.

<portchannel-id>	The range of the port-channel ID is 1 to 64.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
Log Invalid	Displays whether logging of invalid ARP packets is enabled on the VLAN.
ACL Name	The ARP ACL Name, if configured on the VLAN.
Static Flag	If the ARP ACL is configured static on the VLAN.

Default None

Mode Privileged Exec

Display Message

Term	Definition
Interface	The interface ID for each displayed row.
Trust State	Whether the interface is trusted or untrusted for DAI.
Rate Limit	The configured rate limit value in packets per second.
Burst Interval	The configured burst interval value in seconds

3.18.1.4. *Show arp access-list*

This command displays the configured ARP ACLs with the rules. Giving an ARP ACL name as the argument will display only the rules in that ARP ACL.

Format show arp access-list [acl-name]

Term	Definition
<acl-name>	Specifies the ARP ACL name.

Default None

Mode Privileged Exec

3.18.2. Configuration commands

3.18.2.1. *Ip arp inspection validate*

This command enables additional validation checks like source-mac validation, destination-mac validation, and ip address validation on the received ARP packets.

To disable the additional validation checks on the received ARP packets, use the no form of this command.

Format ip arp inspection validate {[src-mac] [dst-mac] [ip]}

no ip arp inspection validate {[src-mac] [dst-mac] [ip]}

Default Disable

Mode Global Config

3.18.2.2. *Ip arp inspection vlan*

This command enables Dynamic ARP Inspection on a list of comma-separated VLAN ranges.

To disable Dynamic ARP Inspection on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection vlan <vlan-list>

no ip arp inspection vlan <vlan-list>

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Disable

Mode Global Config

3.18.2.3. *Ip arp inspection vlan logging*

This command enables logging of invalid ARP packets on a list of comma-separated VLAN ranges.

To disable logging of invalid ARP packets on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection vlan <vlan-list> logging

no ip arp inspection vlan <vlan-list> logging

Term	Definition
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.

Default Enable

Mode Global Config

3.18.2.4. *Ip arp inspection filter*

This command configures the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges. If the static keyword is given, packets that do not match a permit statement are dropped without consulting the DHCP snooping bindings.

To unconfigure the ARP ACL used to filter invalid ARP packets on a list of comma-separated VLAN ranges, use the no form of this command.

Format ip arp inspection filter <acl-name> vlan <vlan-list> [static]

no ip arp inspection filter <acl-name> vlan <vlan-list> [static]

Term	Definition
<acl-name>	Specifies the ARP access-list name up to 31 characters in length.
<vlan-list>	Specifies VLAN ID in a list. The range of VLAN ID is 1 to 4093.
<static>	Specifies ARP ACL is configured static.

Default No ARP ACL is configured on a VLAN

Mode Global Config

3.18.2.5. *Ip arp inspection trust*

This command configures an interface as trusted for Dynamic ARP Inspection.

To configure an interface as untrusted for Dynamic ARP Inspection, use the no form of this command.

Format ip arp inspection trust

no ip arp inspection trust

Default Disable

Mode Interface Config

3.18.2.6. *Ip arp inspection limit*

This command configures the rate limit and burst interval values for an interface. Configuring none for the limit means the interface is not rate limited for Dynamic ARP Inspections.

To set the rate limit and burst interval values for an interface to the default values, use the no form of this command.

Format ip arp inspection limit {rate <pps> [burst interval <seconds>] | none}

no ip arp inspection limit

Term	Definition
<pps>	Specifies rate limit in pps. The range of rate is 0 to 300.
<seconds>	Specifies burst interval in seconds. The range of rate is 1 to 15.

Default 15 pps for rate and 1 second for burst-interval

Mode Interface Config

3.18.2.7. *Arp access-list*

This command creates an ARP ACL.

To delete a configured ARP ACL, use the no form of this command.

Format arp access-list <acl-name>

no arp access-list <acl-name>

Term	Definition
<acl-name>	Specifies the ARP access-list name up to 31 characters in length.

Default None

Mode Global Config

3.18.2.8. *Permit ip host mac host*

This command configures a rule for a valid IP address and MAC address combination used in ARP packet validation.

To delete a rule for a valid IP and MAC combination.

Format permit ip host <sender-ip> mac host <sender-mac>

no permit ip host <sender-ip> mac host <sender-mac>

Term	Definition
<sender-ip>	Specifies IP address in the ARP ACL rule.
<sender-mac>	Specifies MAC address in the ARP ACL rule.

Default None

Mode ARP Access-list Config

3.18.2.9. *Clear ip arp inspection statistics*

This command resets the statistics for Dynamic ARP Inspection on all VLANs.

Format clear ip arp inspection statistics

Default None

Mode Privileged Exec

3.19. Differentiated Service Commands

 This Switching Command function can only be used on the QoS software version.

This chapter contains the CLI commands used for the QoS Differentiated Services (DiffServ) package.

The user configures DiffServ in several stages by specifying:

1. Class

- creating and deleting classes
- defining match criteria for a class

 The only way to remove an individual match criterion from an existing class definition is to delete the class and re-create it.

2. Policy

- creating and deleting policies
- associating classes with a policy
- defining policy statements for a policy/class combination

3. Service

- adding and removing a policy to/from a directional (that is, inbound, outbound) interface

Packets are filtered and processed based on defined criteria. The filtering criteria are defined by a class. The processing is defined by a policy's attributes. Policy attributes may be defined on a per class instance basis, and it is these attributes that are applied when a match occurs.

Packet processing begins by testing the match criteria for a packet. A policy is applied to a packet when a class match within that policy is found.

Note that the type of class - all, any, or acl - has a bearing on the validity of match criteria specified when defining the class. A class type of 'any' processes its match rules in an ordered sequence; additional rules specified for such a class simply extend this list. A class type of ‘acl’ obtains its rule list by interpreting each ACL rule definition at the time the Diffserv class is created. Differences arise when specifying match criteria for a class type 'all', since only one value for each non-excluded match field is allowed within a class definition. If a field is already specified for a class, all subsequent attempts to specify the same field fail, including the cases where a field can be specified multiple ways through alternative formats. The exception to this is when the 'exclude' option is specified, in which case this restriction does not apply to the excluded fields.

The following class restrictions are imposed by the LB8 Series L3 Switch DiffServ design:

- nested class support limited to:

- 'all' within 'all'
- no nested 'not' conditions
- no nested 'acl' class types
- each class contains at most one referenced class

- hierarchical service policies not supported in a class definition
- access list matched by reference only, and must be sole criterion in a class
  - that is, ACL rules copied as class match criteria at time of class creation, with class type 'any'
  - implicit ACL 'deny all' rule also copied
  - no nesting of class type 'acl'

Regarding nested classes, referred to here as class references, a given class definition can contain at most one reference to another class, which can be combined with other match criteria. The referenced class is truly a reference and not a copy, since additions to a referenced class affect all classes that reference it. Changes to any class definition currently referenced by any other class must result in valid class definitions for all derived classes otherwise the change is rejected. A class reference may be removed from a class definition.

The user can display summary and detailed information for classes, policies, and services. All configuration information is accessible via the CLI, and SNMP user interfaces.

3.19.1. General commands

The following characteristics are configurable for the platform as a whole.

3.19.1.1. *Diffserv*

This command sets the DiffServ operational mode to active. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

Format diffsev

Default None

Mode Global Config

3.19.1.2. *No diffserv*

This command sets the DiffServ operational mode to inactive. While disabled, the DiffServ configuration is retained and can be changed, but it is not activated. When enabled, Diffserv services are activated.

Format no diffsev

Default None

Mode Global Config

3.19.2. Class commands

The 'class' command set is used in DiffServ to define:

> **Traffic Classification** specifies Behavior Aggregate (BA) based on DSCP, and Multi- Field (MF) classes of traffic (name, match criteria)
>
> **Service Levels** specifies the BA forwarding classes / service levels. Conceptually, DiffServ is a two-level hierarchy of classes: 1. Service/PHB, 2. Traffic Class

This set of commands consists of class creation/deletion and matching, with the class match commands specifying layer 3, layer 2, and general match criteria. The class match criteria are also known as class rules, with a class definition consisting of one or more rules to identify the traffic belonging to the class. Note that once a class match criterion is created for a class, it cannot be changed or deleted - the entire class must be deleted and re-created.

The CLI command root is ***class-map***.

3.19.2.1. *Class-map*

This command defines a new DiffServ class of type match-all, match-any or match-access-group.

Format class-map [match-all] <class-map-name> [{ipv4 | ipv6}]

Parameter	Description
<class-map-name>	Case sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

When used without any match condition, this command enters the class-map mode. The **<class-map-name>** is the name of an existing DiffServ class.

 The class name 'default' is reserved and is not allowed here. The class type of **match-all** indicates all of the individual match conditions must be true for a packet to be considered a member of the class.

The optional keywords [{ipv4 | ipv6}] specify the Layer 3 protocol for this class. If not specified, this parameter defaults to 'ipv4'. This maintains backward compatibility for configurations defined on systems before IPv6 match items were supported.

The CLI mode is changed to Class-Map Config or Ipv6-Class-Map Config when this command is successfully executed depending on the [{ipv4 | ipv6}] keyword specified.

Default None

Mode Global Config

3.19.2.2. *No class-map*

This command eliminates an existing DiffServ class.

Format no class-map <class-map-name>

Parameter	Description
<class-map-name>	The name of an existing DiffServ class..


The class name 'default' is reserved and is not allowed here. This command may be issued at any time; if the class is currently referenced by one or more policies or by any other class, this deletion attempt shall fail.

Default None

Mode Global Config

3.19.2.3. *Rename*

This command changes the name of a DiffServ class.

Format rename <new-class-map-name>

Parameter	Description
<new-class-map-name>	Case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the class.

 The class name ‘default’ is reserved and must not be used here.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.4. *Match any*

This command adds to the specified class definition a match condition whereby all packets are considered to belong to the class.

Format match any

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.5. *Match class-map*

This command adds to the specified class definition the set of match conditions defined for another class.

Format match class-map <refclassname>

Parameter	Description
<refclassname>	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

 There is no [**not**] option for this match command.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

Restrictions

The class types of both <***classname***> and <***refclassname***> must be identical (that is, any vs. any, or all vs. all). A class type of acl is not supported by this command.

Cannot specify ***<refclassname>*** the same as <***classname***> (that is, self-referencing of class name not allowed). At most one other class may be referenced by a class. Any attempt to delete the <***refclassname***> class while still referenced by any <***classname***> shall fail.

The combined match criteria of <***classname***> and <***refclassname***> must be an allowed combination based on the class type. Any subsequent changes to the <***refclassname***> class match criteria must maintain this validity, or the change attempt shall fail. The total number of class rules formed by the complete reference class chain (includes both predecessor and successor classes) must not exceed a platform-specific maximum. In some cases, each removal of a refclass rule reduces the maximum number of available rules in the class definition by one.

3.19.2.6. *No match class-map*

This command removes from the specified class definition the set of match conditions defined for another class.

Format no match class-map <refclassname>

Parameter	Description
<refclassname>	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

There is no [**not**] option for this match command.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.7. *Match cos*

This command adds to the specified class definition a match condition for the Class of Service value (the only tag in a single tagged packet or the first or outer 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

This command is not available on the Broadcom 5630x platform.

Format match cos <0-7>

Parameter	Description
<0-7>	Integer in the range of 0 to 7 specifying the COS value.

Default None

Mode Class-Map Config

3.19.2.8. *Match secondary-cos*

This command adds to the specified class definition a match condition for the secondary Class of Service value (the inner 802.1Q tag of a double VLAN tagged packet). The value may be from 0 to 7.

Format match secondary-cos <0-7>

Parameter	Description
<0-7>	Integer in the range of 0 to 7 specifying the COS value.

Default None

Mode Class-Map Config

3.19.2.9. *Match destination-address mac*

This command adds to the specified class definition a match condition based on the destination MAC address of a packet. The <address> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <mac-mask> parameter is a layer 2 MAC address bit mask, which need not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

This command is not available on the Broadcom 5630x platform.

Format match destination-address mac <address> <mac-mask>

Parameter	Description
<address>	Specifies any layer 2 MAC address.
<mac-mask>	Specifies a layer 2 MAC address bit mask.

Default None

Mode Class-Map Config

3.19.2.10. *Match dstip*

This command adds to the specified class definition a match condition based on the destination IP address of a packet.

Format match dstip <ipaddr> <ipmask>

Parameter	Description
<ipaddr>	Specifies an IP address.
<ipmask>	Specifies an IP address bit mask; note that although similar to a standard subnet mask, this bit mask need not be contiguous.

Default None

Mode Class-Map Config

3.19.2.11. *Match dstl4port*

This command adds to the specified class definition a match condition based on the destination layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

Format match dstl4port {<port-key> | <0-65535>}

Parameter	Description
<port-key>	To specify the match condition as a single keyword, the value for <**portkey>** is one of the supported port name keywords. The currently supported <**portkey>** values are: **domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www**. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.
<0-65535>	To specify the match condition using a numeric notation, one layer 4 port number is required. The port number is an integer from 0 to 65535. To specify the match condition using a numeric range notation, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.12. *Match ethertype*

This command adds to the specified class definition a match condition based on the value of the ethertype. The <ethertype> value is specified as one of the following keywords: **appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp** or as a custom ethertype value in the range of 0x0600-0xFFFF.

i This command is not available on the Broadcom 5630x platform.

Format match ethertype {<keyword> | <0x0600-0xFFFF>}

Parameter	Description
<keyword>	Specifies appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast etc.
<0x0600-0xFFFF>	Specifies ethertype value.

Default None

Mode Class-Map Config

3.19.2.13. *Match ip dscp*

This command adds to the specified class definition a match condition based on the value of the IP DiffServ Code Point (DSCP) field in a packet, which is defined as the high-order six bits of the Service Type octet in the IP header (the low-order two bits are not checked).

Format match ip dscp <value>

Parameter	Description
<value>	Specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

i The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation. To specify a match on all DSCP values, use the match [not] ip tos <tosbits> <tosmask> command with <**tosbits**> set to 0 and <**tosmask**> set to 03 (hex).

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.14. *Match ip precedence*

This command adds to the specified class definition a match condition based on the value of the IP Precedence field in a packet, which is defined as the high-order three bits of the Service Type octet in the IP header (the low-order five bits are not checked). The precedence value is an integer from 0 to 7.

Format match ip precedence <0-7>

Parameter	Description
<0-7>	Integer from 0 to 7.

i The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

To specify a match on all Precedence values, use the match [not] ip tos <tosbits> <tosmask> command with <**tosbits>** set to 0 and <**tosmask>** set to 1F (hex).

Default None

Mode Class-Map Config

3.19.2.15. *Match ip tos*

This command adds to the specified class definition a match condition based on the value of the IP TOS field in a packet, which is defined as all eight bits of the Service Type octet in the IP header.

Format match ip tos <tosbits> <tosmask>

Parameter	Description
<tosbits>	Two-digit hexadecimal number from 00 to ff.
<tosmask>	Two-digit hexadecimal number from 00 to ff. The <**tosmask>** denotes the bit positions in <**tosbits>** that are used for comparison against the IP TOS field in a packet. For example, to check for an IP TOS value having bits 7 and 5 set and bit 1 clear, where bit 7 is most significant, use a <**tosbits>** value of a0 (hex) and a <**tosmask>** of a2 (hex).

i The ip dscp, ip precedence, and ip tos match conditions are alternative ways to specify a match criterion for the same Service Type field in the IP header, but with a slightly different user notation.

In essence, this the “free form” version of the IP DSCP/Precedence/TOS match specification in that the user has complete control of specifying which bits of the IP Service Type field are checked.

Default None

Mode Class-Map Config

3.19.2.16. *Match protocol*

This command adds to the specified class definition a match condition based on the value of the IP Protocol field in a packet using a single keyword notation or a numeric value notation.

Format match protocol {<protocol-name> | <0-255>}

Parameter	Description
<protocol-name>	One of the supported protocol name keywords . The currently supported values are: **icmp, igmp, ip, tcp, udp**. Note that a value of **ip** is interpreted to match all protocol number values.
<0-255>	To specify the match condition using a numeric value notation, the protocol number is a standard value assigned by IANA and is interpreted as an integer from 0 to 255.

i This command does not validate the protocol number value against the current list defined by IANA.

Default None

Mode Class-Map Config / Ipv6-Class-Map Config

3.19.2.17. *Match source-address mac*

This command adds to the specified class definition a match condition based on the source MAC address of a packet. The <address> parameter is any layer 2 MAC address formatted as six, two-digit hexadecimal numbers separated by colons (e.g., 00:11:22:dd:ee:ff). The <macmask> parameter is a layer 2 MAC address bit mask, which may not be contiguous, and is formatted as six, two-digit hexadecimal numbers separated by colons (e.g., ff:07:23:ff:fe:dc).

This command is not available on the Broadcom 5630x platform.

Format match source-address mac <address> <macmask>

Parameter	Description
<address>	Specifies any layer 2 MAC address.
<macmask>	Specifies a layer 2 MAC address bit mask.

Default None

Mode Class-Map Config

3.19.2.18. *Match scrip*

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Format match srcip <ipaddr> <ipmask>

Parameter	Description
< ipaddr >	Specifies an IP address .
< ipmask >	specifies an IP address bit mask; note that although it resembles a standard subnet mask, this bit mask need not be contiguous.

Default None

Mode Class-Map Config

3.19.2.19. *Match srcl4port*

This command adds to the specified class definition a match condition based on the source layer 4 port of a packet using a single keyword or numeric notation or a numeric range notation.

Format match srcl4port {<port-key> | <0-65535>}

Parameter	Description
<port-key>	One of the supported port name keywords (listed below).

	The currently supported <portkey> values are: domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Each of these translates into its equivalent port number, which is used as both the start and end of a port range.
<0-65535>	To specify the match condition as a numeric value, one layer 4 port number is required. The port number is an integer from 0 to 65535. To specify the match condition as a range, two layer 4 port numbers are required and together they specify a contiguous port range. Each port number is an integer from 0 to 65535, but with the added requirement that the second number be equal to or greater than the first.

Default None

Mode Class-Map Config / IPv6-Class-Map Config

3.19.2.20. *Match vlan*

This command adds to the specified class definition a match condition based on the value of the layer 2 VLAN Identifier field (the only tag in a single tagged packet or the first or outer tag of a double VLAN tagged packet). The VLAN ID is an integer from 1 to 4093.

i This command is not available on the Broadcom 5630x platform.

Format match vlan <1-4093>

Parameter	Description
<1-4093>	The VLAN ID is an integer from 1 to 4093.

Default None

Mode Class-Map Config

3.19.2.21. *Match secondary-vlan*

This command adds to the specified class definition a match condition based on the value of the layer 2 secondary VLAN Identifier field (the inner 802.1Q tag of a double VLAN tagged packet). The VLAN ID is an integer from 1 to 4093.

Format match secondary-vlan <1-4093>

Parameter	Description
<1-4093>	The VLAN ID is an integer from 1 to 4093.

Default None

Mode Class-Map Config

3.19.2.22. *Match dstipv6*

This command adds to the specified class definition a match condition based on the destination IPv6 address of a packet.

Format match dstip6 <destination-ipv6-prefix/prefix-length>

Parameter	Description
<destination-ipv6-prefix/prefix-length>	IPv6 address and prefix length.

Default None

Mode IPv6-Class-Map Config

3.19.2.23. *Match srcipv6*

This command adds to the specified class definition a match condition based on the source IP address of a packet.

Format match srcip6 <source-ipv6-prefix/prefix-length>

Parameter	Description
<source-ipv6-prefix/prefix-length>	IPv6 address and prefix length.

Default None

Mode IPv6-Class-Map Config

3.19.2.24. *Match ip6flowlbl*

This command adds to the specified class definition a match condition based on the IPv6 flow label value.

Format match ip6flowlbl <label>

Parameter	Description
<label>	IPv6 flow label value in the range of 0 to 1048575.

Default None

Mode IPv6-Class-Map Config

3.19.3. Policy commands

The 'policy' command set is used in DiffServ to define:

Traffic Classification Specify traffic conditioning actions (policing, marking, shaping) to apply to traffic classes.

Service Provisioning Specify bandwidth and queue depth management requirements of service levels (EF, AF, etc.).

The policy commands are used to associate a traffic class, which was defined by the class command set, with one or more QoS policy attributes. This association is then assigned to an interface in a particular direction to form a service. The user specifies the policy name when the policy is created.

The DiffServ CLI does not necessarily require that users associate only one traffic class to one policy. In fact, multiple traffic classes can be associated with a single policy, each defining a particular treatment for packets that match the class definition. When a packet satisfies the conditions of more than one class, preference is based on the order in which the classes were added to the policy, with the foremost class taking highest precedence.

This set of commands consists of policy creation/deletion, class addition/removal, and individual policy attributes. Note that the only way to remove an individual policy attribute from a class instance within a policy is to remove the class instance and re-add it to the policy. The values associated with an existing policy attribute can be changed without removing the class instance.

The CLI command root is ***policy-map***.

3.19.3.1. *Assign-queue*

This command modifies the queue id to which the associated traffic stream is assigned. The queueid is an integer from 0 to n-1, where n is the number of egress queues supported by the device.

Format assign-queue <0-7>

Parameter	Description
<0-7>	Queue ID .

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop

3.19.3.2. *Drop*

This command specifies that all packets for the associated traffic stream are to be dropped at ingress.

Format drop

Default None

Mode Policy-Class-Map Config

Incompatibilities Assign Queue, Mark (all forms), Mirror, Police, Redirect

3.19.3.3. *Mirror*

This command specifies that all incoming packets for the associated traffic stream are copied to a specific egress interface (physical port or LAG).

This command is not available on the Broadcom 5630x platform.

Format mirror {<slot/port> | port-channel <port-channel-intf-num>}

Parameter	Description
<slot/port>	Specifies the physical interface where the mirrored packet send to .
<port-channel-intf-num>	Specifies the port-channel interface where the mirrorred packet send to. The range of the port-channel ID is 1 to 64.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Redirect

3.19.3.4. *Redirect*

This command specifies that all incoming packets for the associated traffic stream are redirected to a specific egress interface (physical port or port-channel).

Format redirect {<slot/port> | port-channel <port-channel-intf-num>}

Parameter	Description
<slot/port>	Specifies which physical **i**nterface that traffic stream are redirected to.
<port-channel-intf-num>	Specifies which port-channel interface that traffic stream are directed to. The range of the port-channel ID is 1 to 64.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mirror

3.19.3.5. *Conform-color*

This command is used to enable color-aware traffic policing and define the conform-color class maps used. Used in conjunction with the police command where the fields for the conform level (for simple, single-rate, and two-rate policing) are specified. The <class-map-name> parameter is the name of an existing Diffserv class map, where different ones must be used for the conform and exceed colors.

Format conform-color <class-map-name>

Parameter	Description
<class-map-name>	Name of an existing Diffserv class map, where different ones must be used for the conform colors.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mirror

3.19.3.6. *Mark cos*

This command marks all packets for the associated traffic stream with the specified class of service value in the priority field of the 802.1p header. If the packet does not already contain this header, one is inserted. The CoS value is an integer from 0 to 7.

Format mark cos <0-7>

Parameter	Description
<0-7>	The range of COS value is 0 to 7.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

3.19.3.7. *Mark cos-as-sec-cos*

This command marks outer VLAN tag priority bits of all packets as the inner VLAN tag priority, marking CoS as Secondary CoS. This essentially means that the inner VLAN tag CoS is copied to the outer VLAN tag CoS.

Format mark cos-as-sec-cos

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark IP DSCP, IP Precedence, Police

3.19.3.8. *Class*

This command creates an instance of a class definition within the specified policy for the purpose of defining treatment of the traffic class through subsequent policy attribute statements.

Format class <classname>

Parameter	Description
<classname>	The name of an existing DiffServ class. Note that this command causes the specified policy to create a reference to the class definition.

Default None

Mode Policy-Map Config

3.19.3.9. *No class*

This command deletes the instance of a particular class and its defined treatment from the specified policy.

Format no class <classname>

Parameter	Description
<classname>	The name of an existing DiffServ class. Note that this command removes the reference to the class definition for the specified policy.

Default None

Mode Policy-Map Config

3.19.3.10. *Mark ip-dscp*

This command marks all packets for the associated traffic stream with the specified IP DSCP value.

Format mark ip-dscp <value>

Parameter	Description
<value>	Specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark CoS, Mark IP Precedence, Police

3.19.3.11. *Mark ip-precedence*

This command marks all packets for the associated traffic stream with the specified IP Precedence value. The IP Precedence value is an integer from 0 to 7.

Format mark ip-precedence <0-7>

Parameter	Description
<0-7>	IP precedence value in the range of 0 to 7

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

3.19.3.12. *Police-simple*

This command is used to establish the traffic policing style for the specified class. The simple form of the police command uses a single data rate and burst size, resulting in two outcomes: conform and violate. The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128.

For each outcome, the only possible actions are drop, set-cos-transmit, set-dscp-transmit, setprec-transmit, or transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop.

For set-dscp-transmit, a <dscpval> value is required and is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23,af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

For set-prec-transmit, an IP Precedence value is required and is specified as an integer from 0-7.

For set-cos-transmit an 802.1p priority value is required and is specified as an integer from 0-7.

Format police-simple {<1-4294967295> <1-128> conform-action {drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit }]}

The simple form of the police command uses a single data rate and burst size, resulting in two outcomes:

Parameter	Description
<conform-action & violate-action>	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-dscp-transmit, set-prec-transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.

<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef**.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

Incompatibilities Drop, Mark (all forms)

3.19.3.13. *Police-single-rate*

This command is the single-rate form of the police command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this single-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format police-single-rate {<1-4294967295> <1-128> <1-128> conform-action {drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} exceed-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit }]}

Parameter	Description
<conform-action & violate-action & exceed-action>	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-cos-as-sec-cos , set-dscp-transmit, set-prec-transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured. Besides, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23,**

	af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

3.19.3.14. *Police-two-rate*

This command is the two-rate form of the police command and is used to establish the traffic policing style for the specified class. For each outcome, the only possible actions are drop, set-cos-as-sec-cos, set-cos-transmit, set-sec-cos-transmit, set-dscp-transmit, set-prec-transmit, or transmit. In this two-rate form of the police command, the conform action defaults to send, the exceed action defaults to drop, and the violate action defaults to drop. These actions can be set with this command once the style has been configured.

Format police-two-rate {<1-4294967295> <1-128> <1-4294967295> <1-128> conform-action {drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit} exceed-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit } [violate-action { drop | set-cos-as-sec-cos | set-cos-transmit <0-7> | set-dscp-transmit <value> | set-prec-transmit <0-7> | transmit}]}

Parameter	Description
<conform-action & violate-action & exceed-action>	The conforming data rate is specified in kilobits-per-second (Kbps) and is an integer from 1 to 4294967295. The conforming burst size is specified in kilobytes (KB) and is an integer from 1 to 128. For each outcome, the only possible actions are drop, set-cos-as-sec-cos , set-dscp-transmit, set-prec-transmit, or set-cos-transmit. In this simple form of the police command, the conform action defaults to transmit and the violate action defaults to drop. These actions can be set with this command once the style has been configured. Beside, the set-cos-transmit is to combine only with drop between the conform-action and the violate-action.
<set-cos-transmit>	Priority value is required and is specified as an integer from 0-7.
<set-dscp-transmit>	Required and specified as either an integer from 0 to 63, or symbolically through one of the following keywords: **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef**.
<set-prec-transmit>	IP Precedence value is required and is specified as an integer from 0-7

Default None

Mode Policy-Class-Map Config

3.19.3.15. *Policy-map*

This command establishes a new DiffServ policy. The <policyname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy. The type of policy is specific to the inbound traffic direction as indicated by the in parameter.

Format policy-map <policyname> [{in | out}]

no policy-map <policyname>

Parameter	Description
<policyname>	Policy name up to 31 alphanumeric characters.
no	Delete this policy

Default None

Mode Global Config

3.19.3.16. *Policy-map rename*

This command changes the name of a DiffServ policy. The <policyname> is the name of an existing DiffServ class. The <newpolicyname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the policy.

Format policy-map rename <policyname> <newpolicyname>

Parameter	Description
<policyname>	Old Policy name.
<newpolicyname>	New policy name.

Default None

Mode Global Config

3.19.4. Service commands

The 'service' command set is used in DiffServ to define:

Traffic Classification Assign a DiffServ traffic conditioning policy (as specified by the policy commands) to an interface in the incoming direction.

Service Provisioning Assign a DiffServ service provisioning policy (as specified by the policy commands) to an interface in the outgoing direction.

The service commands attach a defined policy to a directional interface. Only one policy may be assigned at any one time to an interface in a particular direction. The policy type (in, out) must match the interface direction to which it is attached.

This set of commands consists of service addition/removal.

The CLI command root is ***service-policy.***

3.19.4.1. *Service-policy*

This command attaches a policy to an interface in a particular direction.

Format service-policy {in | out} <policy-map-name>

Parameter	Description
<policy-map-name>	The name of an existing DiffServ policy, whose type must match the interface direction. Note that this command causes a service to create a reference to the policy.

i The command can be used in the **Interface Config** mode to attach a policy to a specific interface. Alternatively, the command can be used in the **Global Config** mode to attach this policy to all system interfaces. The direction value is either in or out.

Default None

Mode Global Config, Interface Config

Restrictions Only a single policy may be attached to a particular interface in a particular direction at any one time.

3.19.4.2. *No service-policy*

This command detaches a policy from an interface in a particular direction.

Format no service-policy {in | out} <policy-map-name>

Parameter	Description

<policy-map-name>	The name of an existing DiffServ policy. Note that this command causes a service to remove its reference to the policy.

The command can be used in the **Interface Config** mode to detach a policy from a specific interface. Alternatively, the command can be used in the **Global Config** mode to detach this policy from all system interfaces to which it is currently attached. The direction value is either in or out.

This command effectively disables DiffServ on an interface (in a particular direction).There is no separate interface administrative 'mode' command for DiffServ.

Default None

Mode Global Config, Interface Config

3.19.5. Show commands

The 'show' command set is used in DiffServ to display configuration and status information for:

- Classes
- Policies
- Services

This information can be displayed in either summary or detailed formats. The status information is only shown when the DiffServ administrative mode is enabled; it is suppressed otherwise. There is also a 'show' command for general DiffServ information that is available at any time.

3.19.5.1. *Show class-map*

This command displays all configuration information for the specified class.

Format show class-map [<classname>]

Parameter	Description
<classname>	The name of an existing DiffServ class.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Class Name	The name of this class.
Class Type	The class type (all, any, or acl) indicating how the match criteria are evaluated for this class. A class type of all means every match criterion defined for the class is evaluated simultaneously they must all be true to indicate a class match. For a type of any each match criterion is evaluated sequentially and only one need be true to indicate a class match. Class type acl rules are evaluated in a hybrid manner, with those derived from each ACL Rule grouped and evaluated simultaneously, while each such grouping is evaluated sequentially.
L3 Protocol	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Match Criteria	The Match Criteria fields will only be displayed if they have been configured. They will be displayed in the order entered by the user. These are evaluated in accordance with the class type. The possible Match Criteria fields are: Class of Service, Destination IP Address, Destination Layer 4 Port, Destination MAC Address, Every, IP DSCP, IP Precedence, IP TOS, Protocol Keyword, Reference Class, Source IP Address, Source Layer 4 Port, Source MAC Address, and VLAN.
Values	This field displays the values of the Match Criteria.
Class Name	The name of this class. (Note that the order in which classes are displayed is not necessarily the same order in which they were created.)
Class Type	Class type of 'all' means every match criterion defined for the class is evaluated simultaneously and must all be true to indicate a class match.
Reference Class Name	The name of an existing DiffServ class whose match conditions are being referenced by the specified class definition.

3.19.5.2. *Show diffserv*

This command displays the DiffServ General Status Group information, which includes the current administrative mode setting as well as the current and maximum number of rows in each of the main DiffServ private MIB tables.

Format show diffserv

Default None

Mode Privileged Exec

Display Message

Fields	Definition
DiffServ Admin mode	The current value of the DiffServ administrative mode.
Class Table Size Current/Max	The current or maximum number of entries (rows) in the Class Table.
Class Rule Table Size Current/Max	The current or maximum number of entries (rows) in the Class Rule Table.
Policy Table Size Current/Max	The Layer 3 protocol for this class. Possible values are IPv4 and IPv6.
Policy Instance Table Size Current/Max	The current or maximum number of entries (rows) in the Policy Instance Table.
Policy Attribute Table Size Current/Max	The current or maximum number of entries (rows) in the Policy Attribute Table.
Service Table Size Current/Max	The current or maximum number of entries (rows) in the Service Table.

3.19.5.3. *Show diffserv service*

This command displays policy service information for the specified interface and direction.

Format show diffserv service <slot/port> {in | out}

Parameter	Description
<slot/port>	Specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
DiffServ Admin mode	The current setting of the DiffServ administrative mode. An attached policy is only in effect on an interface while DiffServ is in an enabled mode.
Interface	The slot number and port number of the interface (slot/port).
Direction	The traffic direction of this interface service.

Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

3.19.5.4. *Show diffserv service brief*

This command displays all interfaces in the system to which a DiffServ policy has been attached. The direction parameter is optional; if specified, only services in the indicated direction are shown.

Format show diffserv service brief [in | out]

Default None

Mode Privileged Exec

Display Message

Fields	Definition
DiffServ Admin mode	The current setting of the DiffServ administrative mode. An attached policy is only active on an interface while DiffServ is in an enabled mode.

The following information is repeated for interface and direction (only those

interfaces configured with an attached policy are shown):

Fields	Definition
Interface	The slot number and port number of the interface (slot/port).
Direction	The traffic direction of this interface service.
OperStatus	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

3.19.5.5. *Show policy-map*

This command displays all configuration information for the specified policy.

Format show policy-map [<policy-map-name>]

Parameter	Description

< policy-map-name >	The name of an existing DiffServ policy.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Policy Name	The name of this policy.
Policy Type	The policy type, namely whether it is an inbound or outbound policy definition.

The following information is repeated for each class associated with this policy

(only those policy attributes actually configured are displayed):

Fields	Definition
Class Name	The name of this class.
Mark CoS	Denotes the class of service value that is set in the 802.1p header of outbound packets. This is not displayed if the mark cos was not specified.
Mark IP DSCP	Denotes the mark/re-mark value used as the DSCP for traffic matching this class. This is not displayed if mark ip description is not specified using the police-two-rate command, or if policing is in use for the class under this policy.
Mark IP Precedence	Denotes the mark/re-mark value used as the IP Precedence for traffic matching this class. This is not displayed if either mark DSCP or policing is in use for the class under this policy.
Policing Style	This field denotes the style of policing, if any, used simple.
Committed Rate (Kbps)	This field displays the committed rate, used in simple policing, single-rate policing, and two-rate policing.
Committed Burst Size (KB)	This field displays the committed burst size, used in simple policing.
Conform Action	The current setting for the action taken on a packet considered to conform to the policing parameters. This is not displayed if policing is not in use for the class under this policy.
Conform COS Value	This field shows the priority mark value if the conform action is markcos.

Conform DSCP Value	This field shows the DSCP mark value if the conform action is markdscp.
Conform IP Precedence Value	This field shows the IP Precedence mark value if the conform action is markprec.
Non-Conform Action	The current setting for the action taken on a packet considered to not conform to the policing parameters. This is not displayed if policing not in use for the class under this policy.
Non-Conform DSCP Value	This field displays the DSCP mark value if this action is markdscp.
Non-Conform IP Precedence Value	This field displays the IP Precedence mark value if this action is markprec.
Assign Queue	Directs traffic stream to the specified QoS queue. This allows a traffic classifier to specify which one of the supported hardware queues are used for handling packets belonging to the class.
Drop	Drop a packet upon arrival. This is useful for emulating access control list operation using DiffServ, especially when DiffServ and ACL cannot co-exist on the same interface.
Mirror	Copies a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Redirect	Forces a classified traffic stream to a specified egress port (physical port or LAG). This can occur in addition to any marking or policing action. It may also be specified along with a QoS queue assignment.
Policy Name	The name of this policy. (Note that the order in which the policies are displayed is not necessarily the same order in which they were created.)
Policy Type	The policy type, namely whether it is an inbound or outbound policy definition.
Class Members	List of all class names associated with this policy.

3.19.5.6. *Show policy-map interface*

This command displays policy-oriented statistics information for the specified interface and direction.

Format show policy-map interface {<slot/port> | port-channel <1-64 >} {in | out}

Parameter	Description

<slot/port>	Specifies a valid slot number and port number for the system. The direction parameter indicates the interface direction of interest.
<1-64 >	Specifies the port-channel interface. The range of port-channel ID is 1 to 64.

Default None

Mode Privileged Exec

Display Message

Fields	Definition
Interface	The slot number and port number of the interface (slot/port)
Direction	The traffic direction of this interface service, either in or out.
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface in the indicated direction.

The following information is repeated for each class instance within this policy:

Fields	Definition
Class Name	The name of this class instance.
In Offered Packets	Count of the packets offered to this class instance before the defined DiffServ treatment is applied. Only displayed for the 'in' direction.
In Discarded Packets	Count of the packets discarded for this class instance for any reason due to DiffServ treatment of the traffic class. Only displayed for the 'in' direction.


None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

3.19.5.7. *Show service-policy*

This command displays a summary of policy-oriented statistics information for all interfaces in the specified direction. The direction parameter indicates the interface direction of interest. This command enables or

disables the route reflector client. A route reflector client relies on a route reflector to re-advertise its routes to the entire AS. The possible values for this field are ***enable*** and ***disable.***

Format show service-policy {in | out}

Default None

Mode Privileged Exec

Display Message

The following information is repeated for each interface and direction (only those interfaces configured with an attached policy are shown):

Fields	Definition
Interface	The slot number and port number of the interface (slot/port).
Operational Status	The current operational status of this DiffServ service interface.
Policy Name	The name of the policy attached to the interface.

None of the counters listed here are guaranteed to be supported on all platforms. Only supported counters are shown in the display output.

3.20. ACL Commands

This chapter contains the CLI commands used for showing and configuring MAC Access Control List (ACL) and IP Access Control List (ACL).

3.20.1. Show commands

3.20.1.1. *Show mac access-lists name*

This command displays a MAC access list and all of the rules that are defined for the ACL. The command output varies based on the match criteria configured within the rules of the ACL.

Format show mac access-lists <name>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL to display.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Name	The name of the MAC ACL rule.
Sequence Number	The ordered rule number identifier defined within the ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Source MAC Address	Displays the source MAC address for this rule.
Source MAC Mask	Displays the source MAC mask for this rule.
Destination MAC Address	Displays the destination MAC address for this rule.
Destination MAC Mask	Displays the destination MAC mask for this rule.
Ethertype	Displays the Ethertype keyword or custom value for this rule.
VLAN ID	Displays the VLAN identifier value or range for this rule.
CoS Value	Displays the COS (802.1p) value for this rule.

Assign Queue	Displays the queue identifier to which packets matching this rule are assigned.
Redirect Interface	Displays the slot/port to which packets matching this rule are forwarded.
Mirror Interface	Displays the slot/port to which packets matching this rule are copied.
Time Range Name	Displays the name of the time-range if the MAC ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.
Redirect External AgentId	Indicates whether matching flow packets are allowed to be sent to external applications running alongside NOS on a control CPU.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst size	The committed burst size defined by the rate-limit attribute.

3.20.1.2. *Show mac access-lists*

This command displays a summary of all defined MAC access lists in the system.

Format show mac access-lists

Mode Privileged EXEC

Display Message

Fields	Definition
Current number of all ACLs	The number of user-configured rules defined for this ACL
Maximum number of all ACLs	The maximum number of ACL rules.
MAC ACL Name	The name of the MAC ACL rule.
Rules	The number of rules in this ACL.
Direction	Denotes the direction in which this MAC ACL is attached to the set of interfaces listed. The value is Inbound or Outbound.
Interface(s)	Displays the list of interfaces (slot/port) to which this MAC ACL is attached in a given direction.
VLAN(s)	Displays VLAN(s) to which the MAC ACL applies

3.20.1.3. *Show ip access-lists*

Use this command to view summary information about all IP ACLs configured on the switch. To view more detailed information about a specific access list, specify the ACL number or name that is used to identify the IP ACL.

Format show ip access-lists [<1-199> | <name>]

Parameter	Description
1-199	The ACL ID used to identify a specific IP ACL to display.
name	The ACL name used to identify a specific IP ACL to display.

Default None

Mode Privileged EXEC , User Exec

Display Message

Fields	Definition
Current number of all ACLs	The number of user-configured rules defined for this ACL
Maximum number of all ACLs	The maximum number of ACL rules.
ACL ID/Name	The identifier or Name of this ACL.
Rules	The number of rules configured for the ACL.
Direction	Shows whether the ACL is applied to traffic coming into the interface (ingress) or leaving the interface (egress).
Interface(s)	The interface(s) to which the ACL is applied(ACL interface Bindings)
VLAN(s)	The VLAN(s) to which the ACL is applied(ACL VLAN Bindings)
Sequence Number	The ordered rule number identifier defined within the ACL.
Action	Displays the action associated with each rule. The possible values are Permit or Deny.
Match ALL	Indicates whether this ACL applies to every packet. The possible values are True or False.
IPv4 Protocol	Displays the protocol to filter for this rule.

Source IP Address	Displays the source IP address for this rule.
Source IP Wildcard Mask	Displays the source IP mask for this rule.
Source L4 Port Keyword	Displays the source port for this rule.
Destination IP Address	Displays the destination IP address for this rule.
Destination MAC Mask	Displays the destination IP mask for this rule.
Destination L4 Port Keyword	Displays the destination port for this rule.
IP DSCP	The value specified for IP DSCP.
IP Precedence	The value specified for IP Precedence .
IP TOS	The value specified for IP TOS .
Log	Displays when you enable logging for this rule.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Time Range Name	Displays the name of the time-range if the IP ACL rule has referenced a time range.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Redirect External AgentId	Indicates whether matching flow packets are allowed to be sent to external applications running alongside NOS on a control CPU. AgentId is a unique identifier for the external receive client application. AgentId is an integer in the range 1 to 100. This action will be mutually exclusive with the redirect and mirror actions.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst size	The committed burst size defined by the rate-limit attribute.
Rule Status	Status (Active/Inactive) of the IP ACL rule.

3.20.1.4. *Show access-lists interface*

This command displays ACL information for a designated interface and direction. Use the control-plane keyword to display the ACLs applied on the CPU port.

Format show access-lists interface { { {<slot/port> | port-channel <1-64> } in | out } | control-plane }

Parameter	Description
slot/port	The interface number
1-64	The port-channel ID. The port-channel ID is range from 1 to 64.
in | out	The direction value is either in or out

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Type	The type of access list (IP,IPv6 or MAC)
ACL ID	The identifier of this ACL.
Sequence Number	An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).

3.20.1.5. *Show access-lists vlan*

This command displays ACL information for a particular VLAN ID.

Format show access-lists vlan <vlan-id> {in | out}

Parameter	Description
vlan-id	The VLAN ID
in | out	The direction value is either in or out

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
ACL Type	The type of access list (IP,IPv6 or MAC)
ACL ID	The identifier of this ACL.
Sequence Number	The ordered rule number identifier defined within the ACL.

3.20.2. Configuration commands

3.20.2.1. *Mac access-list extended*

This command creates a MAC access control list (ACL) identified by *name*, consisting of classification fields defined for the Layer 2 header of an Ethernet frame.

If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing ACL.

Format [no] mac access-list extended <name>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
no	Remove this MAC ACL.

Default None

Mode Global Config

3.20.2.2. *Mac access-list extended rename*

This command changes the name of a MAC Access Control List (ACL). The command fails if a MAC ACL by the name *newname* already exists.

Format mac access-list extended rename <oldname> <newname>

Parameter	Description
oldname	The name of an existing MAC ACL to be changed.
newname	New name which uniquely identifies the MAC access list.

Default None

Mode Global Config

3.20.2.3. *Mac access-list resequence*

Use this command to renumber the sequence numbers of the entries for specified MAC access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Format mac access-list resequence {<name>} <1-2147483647> <1-2147483647>

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-2147483647>	The sequence number from which to start. The range is 1-2147483647. The default is 1.
<1-2147483647>	The amount to increment. The range is 1-2147483647. The default is 1.

Default 1

Mode Global Config

3.20.2.4. *Mac access-list*

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list. Note that an implicit 'deny all' MAC rule always terminates the access list.

Note: The 'no' form of this command is not supported, as the rules within an ACL cannot be deleted individually. Rather, the entire ACL must be deleted and re-specified.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The bpdu keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional.

The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported <ethertypekey> values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform.

The mirror parameter allows the traffic matching this rule to be copied to the specified <slot/port>, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified <slot/port> The assign-queue and redirect parameters are only valid for a 'permit' rule.

The time-range parameter allows imposing time limitation on the MAC ACL rule as defined by the parameter time-range-name. If a time range with the specified name does not exist and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the MAC ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Format [1-2147483647] {deny | permit} {{<srcmac> <srcmask>} | any} {{<dstmac> <dstmask>} | any | bpdu} [<ethertypekey> | <0x0600-0xFFFF>] [vlan {{eq <0-4095>}} [cos <0-7>] [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [<rule-id>]

Parameter	Description
1-2147483647	The sequence number of the ACL.
deny | permit	To deny or permit the matching rule.
srcmac srcmask | any	Specifies designated source MAC address and mask pair or any for this rule
destmac destmask | any | bpdu	Specifies designated destination MAC address and mask pair or any or well-known bpdu for this rule
ethertypekey	Appletalk,arp,ibmsna,ipv4,ipv6,ipx,mplsmcast,mplsucast,netbios,novell,pppoe,rarp.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the MAC ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.
portchannel-id	The port channel ID to be mirrored or redirected to.

rule-id	The rule id for the ACL. The allowed value is 1~n, where n is the maximum number of user configurable rules per ACL .

Default None

Mode Mac Access-list Config

To remove the rule with specified ID, use the below **no** form command.

Format no rule <ID>

Parameter	Description
ID	The rule with **ID** to be removed.

Default None

Mode Mac Access-list Config

Format [no] remark <remark>

Parameter	Description
remark	To Add an ACL rule remark
<remark>	The rule ID to be removed.
no	To remove an ACL rule remark

Default None

Mode Mac Access-list Config

3.20.2.5. *Mac access-group*

This command attaches a specific MAC Access Control List (ACL) identified by <name> to an interface, or associates it with a VLAN ID, in a given direction. The <name> parameter must be the name of an existing MAC ACL.

An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not

specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction will be used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The 'Interface Config' mode command is only available on platforms that support independent per-port class of service queue configuration. The VLAN keyword is only valid in the 'Global Config' mode.

 The command with out direction does not apply to the packets generated by own-device. For example, the ping packets from device cannot be filtered by this command with out direction.

Format mac access-group <name> [vlan <vlan-id>] {in |out} [<1-4294967295>]

Parameter	Description
name	The ACL name which is used to identify a specific MAC ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out
1-4294967295	The sequence number of the ACL.

Default None

Mode Global Config
Interface Config

3.20.2.6. *Ip access-list*

Use this command to create an extended IP Access Control List (ACL) identified by <name>, consisting of classification fields defined for the IP header of an IPv4 frame.

If an IP ACL by this name already exists, this command enters IPv4-Access_List config mode to allow updating the existing IP ACL.

Format [no] ip access-list <name>

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

no	Remove this IP ACL identified by <name> from the system.

Default None

Mode Global Config

3.20.2.7. *Ip access-lists rename*

This command changes the name of a IP Access Control List (ACL). The command fails if a IP ACL by the name *newname* already exists. The *newname* must be a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.

Format ip access-list rename <oldname> <newname>

Parameter	Description
oldname	The name of an existing IP ACL to be changed.
newname	New name which uniquely identifies the IP access list.

Default None

Mode Global Config

3.20.2.8. *Ip access-lists resequence*

Use this command to renumber the sequence numbers of the entries for specified IP access list with the given increment value starting from a particular sequence number. The command is used to edit the sequence numbers of ACL rules in the ACL and change the order in which entries are applied. This command is not saved in startup configuration and is not displayed in running configuration.

Format ip access-list resequence {name | id } <1-2147483647> <1-2147483647>

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IP access list.
id	The ACL ID used to identify a specific IP ACL .The value is 1~199.
<1-2147483647>	The sequence number from which to start. The range is 1-2147483647. The default is 1.

<1-2147483647>	The amount to increment.	The range is 1-2147483647. The default is 10.

Default 1

Mode Global Config

3.20.2.9. *Access-list (ip)*

This command creates an IP Access Control List (ACL) that is identified by the access list number, which is 1-99 for standard ACLs or 100-199 for extended ACLs.

Format IP standard ACL

access list <1-99> {remark <remark>} | { [<1-2147483647>] } {deny | permit} {every | <srcip> <srcmask> | host <srcip>} [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [<rule-id>] [redirectExtAgent <agent-id>] [rate-limit <1-4294967295> <1-128>]

Parameter	Description
1-99	The access list number for the IP standard ACL.
remark	Adds a comment (remark) to an IP standard or IP extended ACL.
1-2147483647	Specifies a sequence number for the IP ACL rule. Every rule is assigned a sequence number which is configured by user or generated by the system.
deny | permit	To deny or permit the matching rule.
every	Matches every packet
<srcip> <srcmask>	Specify a source ip address and source netmask pair for the match condition of this IP ACL rule.
host <srcip>	Specify host designated source ip address for this rule.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the IP ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.

portchannel-id	The port channel ID to be mirrored or redirected to.
rule-id	The rule id for the ACL. The allowed value is 1~n, where n is the maximum number of user configurable rules per ACL.
redirectExtAgent <agent-id>	Indicates whether matching flow packets are allowed to be sent to external applications running alongside NOS on a control CPU. <agent-id> is a unique identifier for the external receive client application. <agent-id> is an integer in the range 1 to 100. The *redirectExtAgent* action is mutually exclusive with the *redirect* and *mirror* actions.
rate-limit <1-4294967295> <1-128>	Specifies the allowed rate of traffic as per the configured rate in <1-4294967295> kb/s, and burst-size in <1-128> kilobytes

Mode Global Config

Format IP extended ACL

access list <100-199> {remark <remark>} | { [<1-2147483647>] } {deny | permit} {every | { { <0-255> | eigrp | gre | icmp | igmp | ip | ipinip | ospf | pim | tcp | udp } {<srcip> <srcmask> | any | host <srcip>} [{range {<portkey>|<startport>} {<portkey>|<endport>} } | {eq | neq | lt | gt} {<portkey>|<0-65535>}] {<dstip> <dstmask> | any | host <dstip>} [{range {<portkey>|<startport>} {<portkey>|<endport>} } | {eq | neq | lt | gt} {<portkey>|<0-65535>}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [icmp-type <icmp-type> [icmp-code <icmp-code>] | icmp-message <icmp-message>] [igmp-type <igmp-type>] [dscp <value> | precedence <0-7> | tos <tos> [<tosmask>]] [fragments]} [log] [time-range time-range-name] [assign-queue <queue-id>] [{mirror | redirect} {<slot/port> | port-channel <portchannel-id>}] [<rule-id>] [redirectExtAgent <agent-id>] [rate-limit <1-4294967295> <1-128>]

Parameter	**Description**
100-199	The access list number for the IP extended ACL.
remark	Adds a comment (remark) to an IP standard or IP extended ACL.
1-2147483647	Specifies a sequence number for the IP ACL rule. Every rule is assigned a sequence number which is configured by user or generated by the system.
deny | permit	To deny or permit the matching rule.
every	Matches every packet
{ <0-255> | eigrp | gre | icmp | igmp | ip	Specifies the protocol to filter for an extended IP ACL rule.

| ipinip | ospf | pim | tcp | udp }	
srcip srcmask | any | host	Specifies a source IP address and source netmask pair for matching condition of this rule. The parameter *any* specifies srcip as 0.0.0.0 and srcmask as 255.255.255.255. The parameter *host* A.B.C.D specifies srcip as A.B.C.D and srcmask as 0.0.0.0.
dstip dstmask | any | host	Specifies a destination IP address and netmask pair for matching condition of this rule. The parameter *any* specifies srcip as 0.0.0.0 and srcmask as 255.255.255.255. The parameter *host* A.B.C.D specifies srcip as A.B.C.D and srcmask as 0.0.0.0.
range {<*portkey*> |<*startport*>} {<*portkey*>|<*endport*>}	Specifies the source layer 4 port match condition for the IP ACL rule. You can use the port number ranging from 0-65535 , or specify the *portkey,* which can be one of the following keywords: ● For TCP: bgp,domain,echo,ftp,ftpdata,http,pop2,pop3,smtp,telnet,www. ● For UDP: domain,echo,ntp,rip,snmp,tftp,time,who. For both TCP and UDP, each of these keywords translates into its equivalent port number, which is used as both the start and end of a port range. If the parameter *range* is specified, the IP ACL rule matches only if the layer 4 port number falls within the specified port range. The *startport* and *endport* parameters identify the first and last ports that are parts of the range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the layer 4 port range. Note: This option is available only if the protocol is TCP or UDP.
{eq | neq | lt | gt} {<portkey>|<0-65535>}	Specifies the layer 4 port match condition as comparison form for the rule. You can use the port number ranging from 0-65535, or specify the *portkey.* eq: equal to ; lt: less than ; gt: great than ; neq: not equal to. When *eq* is specified, the IP ACL rule matches only if the layer 4 port number is equal to the specified port number or portkey. When *lt* is specified, IP ACL rule matches only if the layer 4 port number is less than the specified port number or portkey. It is equivalent to specifying the range as 0 to <specified port number-1>.

	When *gt* is specified, the IP ACL rule matches if the layer 4 port number is greater than the specified port number or portkey. It is equivalent to specifying the range as <specified port number+1> to 65535. When *neq* is specified, IP ACL rule matches only if the layer 4 port number is not equal to the specified port number ot portkey. Note: This option is available only if the protocol is TCP or UDP. Port number matches only apply to unfragmented or first fragments.
flag <value>	Specifies that the IP ACL rule matches on the TCP flags. The *value* parameter represents : +fin, -fin, +syn, -syn, +rst, -rst,+psh, -psh, +ack, -ack, +urg, -urg, established. When + is specified, a match occurs if the specified flag is set in the TCP header. When - is specified, a match occurs if the specified flag is NOT set in the TCP header. When established is specified, a match occurs if the specified RST or ACK bits are set in the TCP. Note: This option is available only if the protocol is TCP.
icmp-type <icmp-type> [icmp-code <icmp-code> | icmp-message <icmp-message>]	This option is available only if the protocol is ICMP. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IP ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IP ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: echo, echo-reply, host-redirect, mobile-redirect, net-redirect, net-unreachable, redirect, packet-too-big, port-unreachable, source-quench, router-solicitation, router-advertisement, time-exceeded, ttl-exceeded and unreachable.
igmp-type <igmp-type>	This option is available only if the protocol is IGMP. When igmp-type is specified, the IP ACL rule matches on the specified IGMP message type, a number from 0 to 255.
dscp <value>	Specifies the TOS for an IP ACL rule depending on a match of DSCP value using parameters dscp.
precedence <0-7>	Specifies the TOS for an IP ACL rule depending on a match of precedence values using parameters <0-7>
tos <tos> [<tosmask>]	Specifies the TOS for an IP ACL rule depending on a match value using parameters *tos/tosmask.*

fragments	Specifies that the IP ACL rule matches on fragmented IP packets.
log	Enable logging for this access list rule
time-range-name	Specify the name of the time-range if the IP ACL rule has referenced a time range.
queue-id	Specify the queue identifier to which packets matching this rule are assigned
mirror | redirect	Specify the traffic matching the rule to be copied/redirected to the specific slot/port or port-channel.
slot/port	The interface number to be mirrored or redirected to.
portchannel-id	The port channel ID to be mirrored or redirected to.
rule-id	The rule id for the ACL. The allowed value is 1~n, where n is the maximum number of user configurable rules per ACL.
redirectExtAgent <agent-id>	Indicates whether matching flow packets are allowed to be sent to external applications running alongside NOS on a control CPU. <agent-id> is a unique identifier for the external receive client application. <agent-id> is an integer in the range 1 to 100. The *redirectExtAgent* action is mutually exclusive with the *redirect* and *mirror* actions.
rate-limit <1-4294967295> <1-128>	Specifies the allowed rate of traffic as per the configured rate in <1-4294967295> kb/s, and burst-size in <1-128> kilobytes

Mode Global Config

3.20.2.10. *No access-list*

This command deletes an ACL that is identified by the parameter IP ACL <1-99> *or* <100-199> from the system or remove an ACL rule that is identified by the parameter <1-n> from the an IP ACL <1-99> *or* <100-199>.

Format no access-list {<1-99> | <100-199>} [<rule-id>]

Parameter	Description
1-99	The access list number for the IP standard ACL.
100-199	The access list number for the IP extended ACL.
rule-id	Specifies the access list rule ID. The value is 1~n, where n is the maximum number of user configurable rules per ACL.

Default None

Mode Global Config

3.20.2.11. *Ip access-group*

This command attaches a specified access-control list to an interface, range of interfaces, or all interfaces: or associates it with a VLAN ID in a given direction.

An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode.

 The command with out direction does not apply to the packets generated by own-device. For example, the ping packets from device cannot be filtered by this command with out direction.

Format ip access-group {<1-199> | <name>} [vlan <vlan-id>] {in | out} [<1-4294967295>]

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-199>	The identifier of this ACL. Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out.
1-4294967295	The sequence number of the ACL.

Default None

Mode Global Config
Interface Config

3.20.2.12. *No ip access-group*

This command removes a specified access-control list from an interface, range of interfaces, or all interfaces: or associates it with a VLAN ID in a given direction.

This command specified in 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode setting is applied to all interfaces. The VLAN keyword is only valid in the 'Global Config' mode.

Format no ip access-group {<1-199> | <name>} [vlan <vlan-id>] {in | out}

Parameter	Description
name	The ACL name which is used to identify a specific IP ACL. It is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
<1-199>	The identifier of this ACL. Range 1 to 99 is the access list number for an IP standard ACL. Range 100 to 199 is the access list number for an IP extended ACL.
vlan-id	The VLAN ID. The VLAN keyword is only valid in the 'Global Config' mode.
in | out	The direction value is either in or out.

Default None

Mode Global Config
Interface Config

3.21. IPv6 ACL Commands

3.21.1. Show commands

3.21.1.1. *Show ipv6 access-lists*

This command displays an IPv6 access list and all of the rules that are defined for the IPv6 ACL. Use the [name] parameter to identify a specific IPv6 ACL to display.

Format show ipv6 access-lists [<name>]

Parameter	Description
<name>	ACL name which uniquely identifies the IPv6 ACL to display.

Default None

Mode Privileged EXEC
User EXEC

Display Message

If the "**<name>**" parameter is not specified, the following fields are displayed:

Fields	Definition
Current number of all ACLs	The current number of all ACLs.
Maximum number of all ACLs	The maximum number of all ACLs.
IPv6 ACL Name	The access-list name.
Rules	The number of rules in this ACL.
Direction	The applied direction of the ACL on the interface, inbound or outbound.
Interface(s)	The interfaces which the ACL applied on.
VLAN(s)	The VLAN which the ACL applied on

If the "**<name>**" parameter is specified, the following fields are displayed:

Fields	Definition
ACL Name	The access-list name.

Sequence Number	The ordered rule number identifier defined within the IPv6 ACL.
Action	The action associated with each rule. The possible values are Permit or Deny.
Match Every	Indicates whether this access list applies to every packet. Possible values are True or False.
IPv6 Protocol	The protocol to filter for this rule.
Source IP Address	The source IP address for this rule.
Source L4 Port Keyword	The source port for this rule.
Destination IP Address	The destination IP address for this rule.
Destination L4 Port Keyword	The destination port for this rule.
Fragments	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets or not.
Routing	Specifies that IPv6 ACL rule matches on IPv6 packets that have the routing extension header or not.
IP DSCP	The value specified for IP DSCP.
Flow Label	The value specified for IPv6 Flow Label.
Log	Displays when you enable logging for the rule.
Assign Queue	The queue identifier to which packets matching this rule are assigned.
Mirror Interface	The slot/port to which packets matching this rule are copied.
Redirect Interface	The slot/port to which packets matching this rule are forwarded.
Redirect External AgentId	The agent-id is a unique identifier for the external receive client application . Indicates whether matching flow packets are allowed to be sent to external applications running alongside ICOS on a control CPU.
Time Range Name	Displays the name of the time-range if the Ipv6 ACL rule has referenced a time range.
Rule Status	Status (Active/Inactive) of the MAC ACL rule.
Committed Rate	The committed rate defined by the rate-limit attribute.
Committed Burst	The committed burst size defined by the rate-limit attribute.

3.21.2. Configuration Commands

3.21.2.1. *Ipv6 access-list*

This command creates an IPv6 Access Control List (ACL) identified by <name>, consisting of classification fields defined for the IP header of an IPv6 frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters

uniquely identifying the IPv6 access list.

If an IPv6 ACL by this name already exists, this command enters IPv6-Access-List config mode to allow updating the existing IPv6 ACL.

To delete the IPv6 ACL identified by <name> from the system, use the no form of this command.

Format ipv6 access-list <name>

no ipv6 access-list <name>

Parameter	Description
<name>	access-list name up to 31 characters in length.

Default None

Mode Global Config

The CLI mode changes to IPv6-Access-List Config mode when you successfully execute this command.

3.21.2.2. *Ipv6 access-list rename*

This command changes the name of an IPv6 ACL. The <name> parameter is the name of an existing IPv6 ACL. The <newname> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the IPv6 access list.

This command fails is an IPv6 ACL by the name <newname> already exists.

Format ipv6 access-list rename <oldname> <newname>

Parameter	Description
<oldname>	Current Access Control List name.
<newname>	New Access Control List name.

Default None

Mode Global Config

3.21.2.3. *{deny|permit}*

This command creates a new rule for the current IPv6 access list. Each rule is appended to the list of configured rules for the list.

The 'no' form of this command is not supported, since the rules within an IPv6 ACL cannot be deleted individually. Rather, the entire IPv6 ACL must be deleted and respecified.

An implicit 'deny all' IPv6 rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, either the 'every' keyword or the protocol, source address, and destination address values must be specified. The source and destination IPv6 address fields may be specified using the keyword 'any' to indicate a match on any value in that field. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.

The assign-queue parameter allows specification of a particular hardware queue for handling traffic that matches this rule. The allowed <queue-id> value is 0-(n-1), where n is the number of user configurable queues available for the hardware platform. The assign-queue parameter is valid only for a permit rule.

The mirror parameter allows the traffic matching this rule to be copied to the specified <slot/port>, while the redirect parameter allows the traffic matching this rule to be forwarded to the specified <slot/port>. The assign-queue and redirect parameters are only valid for a permit rule.

The time-range parameter allows imposing time limitation on the IPv6 ACL rule as defined by the parameter time-range-name . If a time range with the specified name does not exist and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied immediately. If a time range with specified name exists and the IPv6 ACL containing this ACL rule is applied to an interface or bound to a VLAN, then the ACL rule is applied when the time-range with specified name becomes active. The ACL rule is removed when the time-range with specified name becomes inactive.

Format {deny | permit} {{every [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>} | {redirectExtAgent <agent-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>]} | {{<0-255> | icmpv6 | ipv6 | tcp | udp} {<source-ipv6-prefix/prefix-length> | any | host <ipv6 srcip>} [eq {<0-65535> | <portkey>}] {<destination-ipv6-prefix/prefix-length> | any | host <ipv6 dstip>} [eq {<0-65535> | <portkey>}] [flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]] [dscp <value>] [flow-label <vlaue>] [icmp-type <icmp-type> [icmp-code <icmp-code>] | icmp-message <icmp-message>] [fragments] [routing] [rule-id] [assign-queue <queue-id>] [log] [{{mirror | redirect} <slot/port> | port-channel <port-channel-group-id>} | {redirectExtAgent <agent-id>}] [rate-limit <1-4294967295> <1-128>] [sequence <1-2147483647>] [time-range <name>] }}

Parameter	Description
deny or permit	Specifies whether the IPv6 ACL rule permits or denies the matching traffic.

every	Specifies to match every packet.
[rule-id]	Specifies a rule ID, the value range from 1 to 1023.
[assign-queue <queue-id>]	Specifies the assign-queue, which is the queue identifier to which packets matching this rule are assigned, the value range from 0 to 7.
[log]	Specifies that this rule is to be logged.
{mirror | redirect} {<slot/port> | port-channel <port-channel-group-id>}	Specifies the mirror or redirect interface which is the unit/slot/port to which packets matching this rule are copied or forwarded, respectively.
redirectExtAgent <agent-id>	Allows matching flow packets to be sent to external applications running alongside ICOS on a control CPU. agent-id is a unique identifier for the external receive client application, the value range from 1 to 100.
rate-limit <rate> <burst-size>	Specifies the allowed rate of traffic as per the configured rate in kbps range from 1 to 4294967295, and burst-size in kbytes range from 1 to 128.
sequence <sequence-number>	Specifies a sequence number for the ACL rule. Every rule receives a sequence number. The sequence number is specified by the user or is generated by the device, the value range from 1 to 2147483647.
time-range <name>	Specifies a time limitation on the ACL rule as defined by the parameter time-range-name.
<0-255>	Specifies the protocol to match for the IPv6 ACL rule, the value range from 0 to 255.
<source-ipv6-prefix/prefix-length>	Specifies a source IPv6 source address and prefix length to match for the IPv6 ACL rule.
<destination-ipv6-prefix/prefix-length>	Specifies a source IPv6 destination address and prefix length to match for the IPv6 ACL rule.
any	Specifying any implies specifying "::/0 "
host <ipv6 srcip>	Specifying host source-ipv6-address implies matching the specified IPv6 address.
host <ipv6 dstip>	Specifying host destination-ipv6-address implies matching the specified IPv6 address.
eq {<0-65535> | <portkey>}	Specifies the layer 4 port match condition for the IPv6 ACL rule. A port number can be used, in the range 0- 65535, or the portkey, which can be one of the following keywords: • For TCP: bgp, domain, echo, ftp, ftp-data, http, smtp, telnet, www, pop2, pop3

	• For UDP: domain, echo, ntp, rip, snmp, tftp, time, who.
flag [+fin | -fin] [+syn | -syn] [+rst | -rst] [+psh | -psh] [+ack | -ack] [+urg | -urg] [established]	Specifies that the IPv6 ACL rule matches on the tcp flags. When +<tcpflagname> is specified, a match occurs if specified <tcpflagname> flag is set in the TCP header. When "-<tcpflagname>" is specified, a match occurs if specified <tcpflagname> flag is *NOT* set in the TCP header. When established is specified, a match occurs if specified either RST or ACK bits are set in the TCP header. Two rules are installed in hardware to when "established" option is specified. This option is visible only if protocol is "tcp".
dscp <value>	Specifies the dscp value to match for for the IPv6 rule. The value range from 0 to 63 or a DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, s1, cs2, cs3, cs4, cs5, cs6, cs7, ef).
flow-label <vlaue>	Specifies the flow-label value to match for for the IPv6 rule. The value range from 0 to 1048575.
icmp-type <icmp-type> [icmp-code <icmp-code> | icmp-message <icmp-message>]	This option is available only if the protocol is ICMPv6. Specifies a match condition for ICMP packets. When *icmp-type* is specified, the IPv6 ACL rule matches on the specified ICMP message type, a number from 0 to 255. When *icmp-code* is specified, the IPv6 ACL rule matches on the specified ICMP message code, a number from 0 to 255. Specifying *icmp-message* implies that both *icmp-type* and *icmp-code* are specified. The following icmp-messages are supported: destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, port-unreachable, router-solicitation, router-advertisement, router-renumbering, time-exceeded, and unreachable. The ICMP message is decoded into the corresponding ICMP type and ICMP code within that ICMP type.
[fragments]	Specifies that IPv6 ACL rule matches on fragmented IPv6 packets (packets that have the next header field set to 44).
[routing]	Specifies that IPv6 ACL rule matches on IPv6 packets that have the routing extension header (the next header field is set to 43).

Default None

Mode IPv6-Access-List Config

3.21.2.4. *Ipv6 traffic-filter*

This command either attaches a specific IPv6 ACL identified by <name> to an interface or associates with a VLAN ID in a given direction. The <name> parameter must be the name of an existing IPv6 ACL.

An optional sequence number may be specified to indicate the order of this mac access list relative to other IPv6 access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specifiedIPv6 access list replaces the currently attached IPv6 access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces. The control-plane and vlan keyword is only valid in the Global Config mode. The Interface Config mode command is only available on platforms that support independent per-port class of service queue configuration.

To remove an IPv6 ACL identified by <name> from the interface(s) in a given direction, use the no form of this command.

Format ipv6 traffic-filter <name> {{control-plane | in | out} | vlan <vlan-id> {in | out}} [<1-4294967295>]

no ipv6 traffic-filter <name> {{control-plane | in | out} | vlan <vlan-id> {in | out}}

Parameter	Description
in|out	The direction value is either in or out.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<1-4294967295>	The sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence. The range of sequence is 1 to 4294967295.

Default None

Mode Global Config

Interface Config

3.22. CoS (Class of Service) Command

3.22.1. Configuration commands

cos-queue strict This command maps an 802.1p priority to an internal traffic class on a "per-port" basis.

Format cos-queue strict <0-7> <0-7>

no queue cos-map

Parameter	Description
<0-7>	The range of queue priority is 0 to 7.
<**0-7>**	The range of mapped traffic class is 0 to 7**.**
no	Reset to the default mapping of the queue priority and the mapped traffic class.

Default None

Mode Interface Config

cos-queue min-bandwidth This command specifies the minimum transmission bandwidth guarantee for each interface queue.

Format cos-queue min-bandwidth <bw-0> <bw-1> ⋯ <bw-7>

no queue cos-queue min-bandwidth

Parameter	Description
<bw-0> <bw-1> ... <bw-7>	Each Valid range is (0 to 100) in increments of 5 and the total sum is less than or equal to 100.
no	Restores the default for each queue's minimum bandwidth value.

Default None

Mode Interface Config

cos-queue strict This command activates the strict priority scheduler mode for each specified queue on a "per-port" basis.

Format cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>]

no cos-queue strict <queue-id-0> [<queue-id-1> … <queue-id-7>]

Parameter	Description
<queue-id>	Queue ID from 0 to 7.
no	Restores the default weighted scheduler mode for each specified queue on a "per-port" basis.

Default None

Mode Interface Config

3.23. Domain Name Server Relay Commands

3.23.1. Show hosts

This command displays the static host name-to-address mapping table.

Format show hosts

Default None

Mode Privileged Exec

Display Message

Parameter	Definition
Host Name	Domain host name.
Default Domain	Default domain name.

Default Domain List	Default domain list.
Domain Name Lookup	DNS client enabled/disabled.
Number of Retries	Number of time to retry sending DNS queries.
Retry Timeout Period	Amount of time to wait for a response to a DNS query.
Name Servers	Configured name servers.

Example: The following shows examples of the CLI display output for the commands.

(Pakedge-MS-1212-189667) (Config)#show hosts

Host name.....
Default domain..... Domain name is not configured
Default domain list..... .corp
Domain Name Lookup..... Enabled
Number of retries..... 2
Retry timeout period..... 3
Name servers (Preference order)..... 10.243.16.11, 10.243.17.11

Dns Client Source Interface..... (not configured)

Configured host name-to-address mapping:

Host	Addresses
test	10.1.1.1

Host	Total	Elapsed	Type	Addresses

No hostname is mapped to an IP address

3.23.2. Ip host

This command creates a static entry in the DNS table that maps a host name to an IP address.

Format ip host <name> <ipaddr>

Parameter	Definition
<name>	Host name.
<ipaddr>	IPv4 address of the host.

Default None

Mode Global Config

no ip host

Remove the corresponding name to IP address mapping entry.

Format no ip host <name>

Mode Global Config

3.23.3. Clear host

This command clears the entire static host name-to-address mapping table.

Format clear host <hostname | all>

Default None

Mode Privileged Exec

3.23.4. Ip domainname

This command defines the default domain name to be appended to incomplete host names (i.e., host names passed from a client are not formatted with dotted notation).

Format ip domainname <name>

Parameter	Definition
<name>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-64 characters)

Default None

Mode Global Config

no ip domainname

Remove the default domain name.

Format no ip domainname <name>

Mode Global Config

3.23.5. Ip domainlist

This command defines the domain name that can be appended to incomplete host names (i.e., host names passed from a client are not formatted with dotted notation).

Format ip domainlist <name>

Parameter	Definition
<name>	Default domain name used to complete unqualified host names. Do not include the initial period that separates an unqualified name from the domain name. (Range: 1-64 characters)

Default None

Mode Global Config

3.23.6. Ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution.

Note: The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

Format ip name-server <ipaddr>

Parameter	Definition
<ipaddr>	IP address of the Domain Name Servers.

Default None

Mode Global Config

no ip name-server

Remove the corresponding Domain Name Server entry from the table.

Format no ip name-server <ipaddr>

Mode Global Config

3.23.7. Ip name server

This command specifies the source address of dns client to use for name-to-address resolution.

Format ip name server { server-address1 …server-address8}

Parameter	Definition
server-address1 .. 8	Specifies the dns server address

Default None

Mode Global Config

no ip name server

This command will reset the DNS source interface to the default settings.

Format no ip name server source-interface

Mode Global Config

3.23.8. Ip domain lookup

This command enables the IP Domain Naming System (DNS)-based host name-to-address translation.

Format ip domain lookup

Default None

Mode Global Config

no ip domain lookup

This command disables the IP Domain Naming System (DNS)-based host name-to-address translation.

Format no ip domain lookup

Mode Global Config

3.23.9. Ip domain retry

This command specifies the number of times to retry sending Domain Name System (DNS) queries.

Format ip domainretry <0-100>

Parameter	Definition
<0-100>	The number of times to retry sending a DNS query to the server.

Default 2

Mode Global Config

no ip domain retry

This command will reset the number of retry times to the default settings.

Format no ip domainretry

Mode Global Config

3.23.10. Ip domain timeout

This command specifies the amount of time to wait for a response to a DNS query.

Format ip domain timeout <0-3600>

Default 3

Mode Global Config

no ip domain timeout

This command will reset the timeout to the default setting.

Format no ip domain timeout

Mode Global Config

3.24. Time Zone Commands

This command sets the system time and date.

The x86 platforms rely on the Linux NTP to manage the time zone and the time of day. The NTP is configured outside of NOS. NOS for x86 does not include the internal SNTP client and does not support SNTP commands and Time Zone clock commands.

System time and date cannot be configured when SNTP is enabled. The SNTP clock takes precedence over the configured system time and date if SNTP is enabled after you configure the system time and date.

3.24.1. Clock summer-time date

Use this command to set the Daylight Saving Time (DST), also known as summertime, offset to UTC. You have toe specify the start year and end year along with the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format clock summer-time date {<date> <month> <year> <hh:mm> <date> <month> <year> <hh:mm>} [offset <offset>] [zone <acronym>]

Parameter	Definition
date	Day of the month. The range is 1 to 31.
month	Month, and the range is the first three letters of month spelling (for example, Jan).
year	Year, and the renage is 2000 to 2097.
hh:mm	Time in 24-hour format in hours and minutes. “hh” range is 0 to 23 and “mm” range is 0 to 59.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Default None

Mode Global Config

3.24.2. Clock summer-time recurring

Use this command to set summertime offset to UTC recursively every year. This means that summertime will affect every year from the time of configuration. You have toe specify the start year and end year along with the month, day, and time. If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format clock summer-time recurring {<week> <day> <month> <hh:mm> <week> <day> <month> <hh:mm> | <EU> | <USA>} [offset <offset>] [zone <acronym>]

Parameter	Definition
week	Week of the month. The range is 1 to 5, first, and last.
day	Day of the week. The range is the first three letters by name of day; sun, for example.
month	Month, and the range is the first three letters of month spelling (for example, Jan).
hh:mm	Time in 24-hour format in hours and minutes. “hh” range is 0 to 23 and “mm” range is 0 to 59.
EU	The system clock uses the standard recurring daylight saving time settings used in countries in the European Union.
USA	The system clock uses the standard recurring daylight saving time settings used in United States.
offset	The number of minutes to add during the summertime. The range is 1 to 1440.
acronym	The acronym for the time zone to be displayed when summertime is in effect. The range is up to four characters.

Default None

Mode Global Config

no clock summer-time

Use this command to reset the summertime configuration.

Format no clock summer-time

Mode Global Config

3.24.3. Clock timezone

Use this command to set the offset to Coordinated Universal Time (UTC). If the optional parameters are not specified, they are read as either zero (0) or \0, as appropriate.

Format clock timezone {hours} [minutes <minutes>] [zone <acronym>]

Parameter	Definition
hours	Hours difference from UTC. The range is -12 to 13.
Minutes	Minutes difference from UTC. The range is zero (0) to 59.
acronym	The acronym for the time zone. The range is up to four characters.

Default None

Mode Global Config

4. Routing Commands

4.1. Address Resolution Protocol (ARP) Commands

4.1.1. Show commands

4.1.1.1. *Show arp*

This command displays the Address Resolution Protocol (ARP) cache.

Format show arp

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Age Time	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic renew mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they aged out.
Total Entry Count Current/Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Configured/Active/Max	Field listing configured static entry count, active static entry count, and maximum static entry count in the ARP table.

The following are displayed for each ARP entry.

Fields	Definition

IP Address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC Address	Is the hardware MAC address of that device.
Interface	Is the routing slot/port associated with the device ARP entry.
Type	Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.
Age	This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format).

4.1.1.2. *Show arp brief*

This command displays the brief Address Resolution Protocol (ARP) table information.

Format show arp brief

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Age Time	Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.
Response Time	Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.
Retries	Is the maximum number of times an ARP request is retried. This value was configured into the unit.
Cache Size	Is the maximum number of entries in the ARP table. This value was configured into the unit.
Dynamic renew mode	Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they aged out.
Total Entry Count Current/Peak	Field listing the total entries in the ARP table and the peak entry count in the ARP table.
Static Entry Count Configured/Active/Max	Field listing configured static entry count, active static entry count, and maximum static entry count in the ARP table.

4.1.1.3. *Show arp switch*

This command displays the static Address Resolution Protocol (ARP) table information.

Format show arp switch

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
IP address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC address	Is the MAC address for that device.

4.1.2. Configuration commands

4.1.2.1. *Arp*

This command creates an ARP entry. The value for <ipaddress> is the IP address of a device on a subnet attached to an existing routing interface. The value for <macaddress> is a unicast MAC address for that device.

Format arp <ipaddr> <macaddr>

no arp <ipaddr> <macaddr>

Fields	Definition
IP address	Is the IP address of a device on a subnet attached to an existing routing interface.
MAC address	Is a MAC address for that device. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example, 00:06:29:32:81:40.
no	This command deletes an ARP entry.

Default None

Mode Global Config

4.1.2.2. *Arp cachesize*

This command configures the maximum number of entries in the ARP cache. The ARP cache size value is platform dependency.

Format arp cachesize <1152-8192> or arp cachesize <1152-6144>

no arp cachesize

Fields	Definition
<1152-8192>	The range of cache size is 1152 to 8192 for the following platform • ipv4-routing data-center default • ipv4-routing dcvpn-data-center • dual-ipv4-and-ipv6 default • dual-ipv4-and-ipv6 alpm • dual-ipv4-and-ipv6 alpm-mpls-data-center • dual-ipv4-and-ipv6 data-center • dual-ipv4-and-ipv6 dcvpn-data-center • dual-ipv4-and-ipv6 mpls-data-center
<1152-6144>	The range of cache size is 1152 to 6144 for the following platform: • ipv4-routing default • ipv4-routing data-center plus
no	This command configures the default ARP cache size.

Default The default cache size is 8192 or 6144, which depends on the platform currently used.

Mode Global Config

4.1.2.3. *Arp dynamicrenew*

This command enables ARP component to automatically renew ARP entries of type dynamic when they age out.

Format arp dynamicrenew

no arp dynamicrenew

Fields	Definition

no	This command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Default None

Mode Global Config

4.1.2.4. *Arp resptime*

This command configures the ARP request response timeout.

Format arp resptime <1-10>

no arp resptime

Fields	Definition
<1-10>	The range of default response time is 1 to 10 seconds.
no	This command configures the default response timeout time.

Default The default response time is 1.

Mode Global Config

4.1.2.5. *Arp retries*

This command configures the ARP count of maximum request for retries.

Format arp retries <0-10>

no arp retries

Fields	Definition
<1-10>	The range of maximum request for retries is 0 to 10.
no	This command configures the default count of maximum request for retries.

Default The default value is 4.

Mode Global Config

4.1.2.6. *Arp Timeout*

This command configures the ARP entry ageout time.

Format arp timeout <15-21600>

no arp timeout

Fields	Definition
<15-21600>	Represents the IP ARP entry ageout time in seconds. The range is 15 to 21600 seconds.
no	This command configures the default ageout time for IP ARP entry.

Default The default value is 1200.

Mode Global Config

4.1.2.7. *Clear arp-cache*

This command causes all ARP entries of type dynamic to be removed form the ARP cache. If the [gateway] parameter is specified, the dynamic entries of type gateway are purged as well.

Format clear arp-cache [gateway | interface {<slot/port> | vlan <vlan-id>}]

Default None

Mode Privileged Exec

4.2. IP Routing Commands

4.2.1. Show commands

4.2.1.1. *Show ip brief*

This command displays all the summary information of the IP.

Format show ip brief

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Default Time to Live	The computed TTL (Time to Live) of forwarding a packet from the local router to the final destination.
Maximum Next Hops	The maximum number of hops supported by this switch.
Maximum Routes	The maximum number of routes the packet can travel.
ICMP Rate Limit Interval	Shows how often the token bucket is initialized with burst-size tokens. Burst-interval is from 0 to 2147483647 milliseconds. The default burst-interval is 1000 msec.
ICMP Rate Limit Burst Size	Shows the number of ICMPv4 error messages that can be sent during one burst-interval. The range is from 1 to 200 messages. The default value is 100 messages.
ICMP Echo Replies	Shows whether ICMP Echo Replies are enabled or disabled.
ICMP Redirects	Shows whether ICMP Redirects are enabled or disabled.
Dead Gateway Detection	Show whether Dead Gateway Detection is enabled or disabled.
Dead Gateway Detection Probe Interval	Shows the interval that ARP request is sent.

4.2.1.2. *Show ip interface*

This command displays all pertinent information about the IP interfaces.

Format show ip interface <slot/port>

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command “ip helper-address (Interface Config)”
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.
Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface. Active State Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.

IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

4.2.1.3. *Show ip interface vlan*

This command displays all pertinent information about the VLAN routing interfaces.

Format show ip interface vlan <1-4093>

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Routing Interface Status	Determine the operational status of IPv4 routing Interface. The possible values are Up or Down.
Primary IP Address	The primary IP address and subnet masks for the interface. This value appears only if you configure it.
Method	Shows whether the IP address was configured manually or acquired from a DHCP server.
Secondary IP Address	One or more secondary IP addresses and subnet masks for the interface. This value appears only if you configure it.
Helper IP Address	The helper IP addresses configured by the command “ip helper-address (Interface Config)”
Routing Mode	The administrative mode of router interface participation. The possible values are enable or disable. This value is configurable.
Administrative Mode	The administrative mode of the specified interface. The possible values of this field are enable or disable. This value is configurable.
Forward Net Directed Broadcasts	Displays whether forwarding of network-directed broadcasts is enabled or disabled. This value is configurable.

Proxy ARP	Displays whether Proxy ARP is enabled or disabled on the system.
Local Proxy ARP	Displays whether Local Proxy ARP is enabled or disabled on the interface. Active State displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.
Link Speed Data Rate	An integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).
MAC Address	The burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.
Encapsulation Type	The encapsulation type for the specified interface. The types are: Ethernet or SNAP.
IP MTU	The maximum transmission unit (MTU) size of a frame, in bytes.
Bandwidth	Shows the bandwidth of the interface.
Destination Unreachables	Displays whether ICMP Destination Unreachables may be sent (enabled or disabled).
ICMP Redirects	Displays whether ICMP Redirects may be sent (enabled or disabled).

4.2.1.4. *Show ip interface brief*

This command displays summary information about IP configuration settings for all ports in the router.

Format show ip interface brief

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Interface	Valid slot, and port number separated by forward slashes or VLAN routing interface.
State	Indicate the operational state of the routing interface.
IP Address	The IP address of the routing interface.

IP Mask	The IP mask of the routing interface.
Method	Is the way to get the IP Address. The possible value is “Manual”, “DHCP” or “None”.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

4.2.1.5. *Show ip route*

This command displays the routing table. The <ip-address> specifies the network for which the route is to be displayed and displays the best matching best-route for the address. The <mask> specifies the subnet mask for the given <ip-address>. When you use the <longer-prefixes> keyword, the <ip-address> and <mask> pair becomes the prefix, and the command displays the routes to the addresses that match that prefix. Use the **<protocol>** parameter to specify the protocol that installed the routes. The value for **<protocol>** can be **connected, bgp, ospf, or static**. Use the <all> parameter to display all routes including best and nonbest routes. If you do not use the <all> parameter, the command only displays the best route.

If you use the <connected> keyword for **<protocol>**, the all option is not available because there are no best or non-best connected routes.

Format show ip route [{<ip-address> [<protocol>] | {<ip-address> <mask> [longer-prefixes] [<protocol>] | <protocol>} [all] | all}]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output. Route Codes: R - RIP Derived, O - OSPF Derived, C - Connected, S - Static B - BGP Derived, IA - OSPF Inter Area E1 - OSPF External Type 1, E2 - OSPF External Type 2 N1 - OSPF NSSA External Type 1, N2 - OSPF NSSA External Type 2 S U - Unnumbered Peer L - Leaked Route, K - Kernel, D - Database Route

State	Indicate the operational state of the routing interface.
IP Address	The IP address of the routing interface.
IP Mask	The IP mask of the routing interface.
Method	Is the way to get the IP Address. The possible value is “Manual”, “DHCP” or “None”.
Netdir Bcast	Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.
MultiCast Fwd	Indicates the multicast forwarding administrative mode on the interface. Possible values are Enable or Disable.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

4.2.1.6. *Show ip route connected*

This command displays directly connected routes.

Format show ip route connected

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

4.2.1.7. *Show ip route static*

This command displays Static Routes. The option **all** command displays all (best and non-best) routes.

Format show ip route static [all]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.
IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

4.2.1.8. *Show ip route hw-failure*

This command displays the routes that failed to be added to the hardware due to the hash errors or a table full condition.

Format show ip route hw-failure

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Route Codes	Displays the key for the routing protocol codes that might appear in the routing table output.

The command displays the routing tables in the following format:

Code IP-Address/Mask [Preference/Metric] via Next-Hop, Interface

Fields	Definition
Code	The codes for the routing protocols that created the routes.

IP-Address/Mask	The IP-Address and mask of the destination network corresponding to this route.
Preference	The administrative distance associated with this route. Routes with low values are preferred over routes with higher values.
Metric	The cost associated with this route.
via Next-Hop	The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.
Interface	The outgoing router interface to use when forwarding traffic to the next destination.

4.2.1.9. *Show ip route summary*

This command displays the routing table summary. Use the optional **all** parameter to show the number of all routes, including best and non-best routes. To include only the number of best routes, do not use the optional parameter.

Format show ip route summary [all]

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Connected Routes	The total number of connected routes in the routing table.
Static Routes	Total number of static routes in the routing table.
BGP Routes	Total number of routes installed by BGP protocol.
External	The number of external BGP routes.
Internal	The number of internal BGP routes.
Local	The number of local BGP routes.
OSPF Routes	Total number of routes installed by OSPF protocol: **Intra Area Routes**: Total number of Intra Area routes installed by OSPF protocol.

	Inter Area Routes: Total number of Inter Area routes installed by OSPF protocol. **External Type-1 Routes**: Total number of External Type-1 routes installed by OSPF protocol. **External Type-2 Routes**: Total number of External Type-2 routes installed by OSPF protocol.
Reject Routes	Total number of reject routes installed by all protocols.
Total Routes	Total number of routes in the routing table.
Best Routes (High)	The number of best routes currently in the routing table. This number only counts the best route to each destination. The value in parentheses indicates the highest count of unique best routes after counters were last cleared.
Alternate Routes	The number of alternate routes currently in the routing table. An alternate route is a route that was not selected as the best route to its destination.
Route Adds	The number of routes that have been added to the routing table.
Route Modifies	The number of routes that have been changed after they were initially added to the routing table.
Route Deletes	The number of routes that have been deleted from the routing table.
Unresolved Route Adds	The number of route adds that failed because none of the route's next hop were on a local subnet. Note that static routes can fail to be added to the routing table at startup because ther routing interfaces are not yet up. This counter gets incremented in this case. The static routes are added to the routing table when the routing interfaces come up.
Invalid Route Adds	The number of routes that failed to be added to the routing table because the route was invalid. A log message is written for each of these failures.
Failed Route Adds	The number of routes that failed to be added to the routing table because of a resource limitation in the routing table.
Hardware Failed Route Adds	The number of routes failed to be inserted into the hardware because of a hash error or a table full condition.
Reserved Locals	The number of routing table entries reserved for a local subnet on a routing interface that is down. Space for local routes is always reserved so that the local routes can be installed when a routing interface is up.
Unique Next Hop (High)	The number of the distinct next hops used among all routes currently in the routing table. This number includes local interfaces for local routes and neighbors for indirect routes. The value in the parentheses indicates the highest count of unique next hops after counters were last cleared.

Next Hop Groups (High)	The current number of next hop groups in use by one or more routes. Each next hop group includes one or more next hops. The value in the parentheses indicates the highest count of next hop groups after counters were last cleared.
ECMP Groups (High)	The number of next hop groups with multiple next hops. The value in the parentheses indicates the highest count of next hop groups after counters were last cleared.
ECMP Routes	The number of routes with multiple next hops currently in the routing table.
Truncated ECMP Routes	The number of ECMP routes that are currently installed in the forwarding table with just one next hop. The forwarding table may limit the number of ECMP routes or the number of ECMP groups. When an ECMP route cannot be installed because such a limit is reached, the route is installed with a single next hop.
ECMP Retries	The number of ECMP routes that have been installed in the forwarding table after initially being installed with a single next hop.
Routes with n Next Hop	The current number of routes with specific number (n) of next hops.

4.2.1.10. *Clear ip route counters*

This command resets the IPv4 routing table counters reported in the command “show ip route summary” to zero. This command only resets event counters. Counters that report the current state of the routing table, such as the number of routes of each type, are not reset.

Format clear ip route counters

Default None

Mode Privileged EXEC

4.2.1.11. *Show ip stats*

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format show ip stats

Default None

Mode Privileged EXEC

4.2.1.12. *Show routing heap summary*

This command displays a summary of the memory allocation from the routing heap. The routing heap is a chunk of memory set aside when the system boots for use by the routing protocols.

Format show routing heap summary

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
Heap Size	The amount of memory, in bytes, allocated at startup for the routing heap.
Memory in Use	The number of bytes currently allocated.
Memory on Free List	The number of bytes currently on the free list. When a chunk of memory from the routing heap is freed, it is placed on a free list for future reuse.
Memory Available in Heap	The number of bytes in the original heap that have never been allocated.
In Use High Water Mark	The maximum memory in use since the system last rebooted.

4.2.2. Configuration commands

4.2.2.1. *Routing*

This command enables routing for an interface.

Format routing
no routing

Fields	Definition
no	Disable routing for an interface.

Default Disable

Mode Interface Config

4.2.2.2. *Ip routing*

This command enables the IP Router Admin Mode for the master switch.

Format ip routing
no ip routing

Fields	Definition
no	Disable the IP Router Admin Mode for the master switch.

Default Disable

Mode Global Config

4.2.2.3. *Ip address*

This command configures an IP address on an interface. The IP address may be a secondary IP address.

Format ip address <ipaddr> {<subnet-mask> | <prefix-lengh>} [secondary]
no ip address <ipaddr> <subnet-mask> [secondary]

Fields	Definition
<ipaddr>	IP address of the interface.
<subnet-mask>	Subnet mask of the interface.
<prefix-lengh>	Implements RFC 3021 via using the / notation of the subnet mask. This integer indicates the length of the subnet mask. Range is from 1 to 31.
[secondary]	It is a secondary IP address.
no	Delete an IP address from an interface.

Default None

Mode Interface Config

4.2.2.4. *Ip address dhcp*

This command enables the DHCPv4 client on an in-band interface so that it can acquire network information, such as the IP address, subnet mask, and default gateway, from a network DHCP server. When

DHCP is enabled on the interface, the system automatically deletes all manually configured IPv4 addresses on the interface.

To enable the DHCPv4 client on an in-band interface and send DHCP client messages with the client identifier option (DHCP Option 61), use the **ip address dhcp client-id** command in interface configuration mode.

Format ip address dhcp {[restart] | [client-id]}

no ip address dhcp [client-id]

Fields	Definition
[restart]	To restart the DHCPv4 client to acquire an IP Address from DHCP server.
[client-id]	To send the DHCPv4 messages with the DHCP client identifier.
no	This command releases a leased address and disables DHCPv4 on an interface.

Default Disable

Mode Interface Config

4.2.2.5. *Ip default-gateway*

This command manually configures a global default gateway address. Only one default gateway can be configured. If you invoke this command several times, each command replaces the previous configuration.

Format ip default-gateway <ipaddr>

no ip default-gateway

Fields	Definition
<ipaddr>	A valid IPv4 address.
no	Remove the default gateway address from the configuration.

Default None

Mode Global Config

4.2.2.6. *Ip load-sharing*

This command manually configures the IP ECMP load balancing mode.

Format ip load-sharing <1-6> {inner | outer}

no ip load-sharing

Fields	Definition
<1 - 6>	The load balancing or sharing mode for all ECMP groups. 1: Based on a hash using the Source IP address of the packet. 2: Based on a hash using the Destination IP address of the packet. 3: Based on a hash using the Source and Destination IP addresses of the packet. 4: Based on a hash using the Source IP address and the Source TCP/UDP Port field of the packet. 5: Based on a hash using the Destination IP address and the Destination TCP/UDP Port field of the packet. 6: Based on a hash using the Source and Destination IP address, and the Source and Destination TCP/UDP Port fields of the packet.
no	Reset the load balancing or sharing mode to the default mode, 6.

Default 6

Mode Global Config

4.2.2.7. *Ip route*

This command configures a static route. Use the optional *vrf* parameter to configure the static route in the specified virtual router instance.

Format ip route [vrf <vrf-name>] <networkaddr> <subnetmask> [{<nexthopip> | Null0} {{[<1-255 >] description <description>} | description <description>}]

no ip route <networkaddr> <subnetmask> [{{<nexthopip> [<1-255 > | description]} | {Null0 [<1-255 > | description]}}]

Fields	Definition
<vrf-name>	Specify the name of the VRF in which this static route is installed.
<networkaddr>	A valid IP address.
<subnetmask>	A valid subnet mask.

<nexthopip>	IP address of the next hop router.
<1-255>	The preference value of this route. The range is 1 to 255.
<description>	The description for the route.
Null0	Null interface.
no	Delete all next hops to a destination static route. If the optional <nextHopRtr> parameter is designated, the next hop is deleted and if the optional preference value is designated, the preference value of the static route is reset to its default value, 1.

Default None

Mode Global Config

4.2.2.8. *Ip route default*

This command configures the default route. Use the optional *vrf* parameter to configure the static route in the specified virtual router instance.

Format ip route [vrf <vrf-name>] default <nexthopip> [1-255]

Fields	Definition
vrf-name	Specify the name of the VRF in which this static route is installed.
<nexthopip>	IP address of the next hop router.
<1-255>	Precedence value of this route.

Default None

Mode Global Config

4.2.2.9. *Ip route distance*

This command sets the default distance (preference) for static routes. Use the optional *vrf* parameter to configure the default distance (preference) for static routes in the specified virtual router instance.

Lower route distance values are preferred when determining the best route. The ip route and ip route default commands allow you to optionally set the distance (preference) of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default

distance. The new default distance will only be applied to static routes created after invoking the ip route distance command.

Format ip route [vrf <vrf-name>] distance <1-255>

Fields	Definition
vrf-name	Specify the name of the VRF in which this static route is installed.
<1-255>	Default the Distance value of static routes. The range is 1 to 255.

Default The default preference value is 1

Mode Global Config

4.2.2.10. *Ip mtu*

This command sets the IP Maximum Transmission Unit (MTU) on a routing interface or range of interfaces. The IP MTU is the size of the largest IP packet that can be transmitted on the interface without fragmentation. Forwarded packets are dropped if they exceed the IP MTU of the outgoing interface.

Packets originated on the router, such as OSPF packets, may be fragmented by the IP stack.

OSPF advertises the IP MTU in the Database Description packets it sends to its neighbors during database exchange. If two OSPF neighbors advertise different IP MTUs, they will not form an adjacency. (unless OSPF has been instructed to ignore differences in IP MTU with the ip ospf mtu-ignore command.)

Format ip mtu <68-9198>

no ip mtu <68-9198>

Fields	Definition
<68-12270>	The IP MTU on a routing interface. The range is 68 to 9198.
no	Reset the ip mtu to the default value.

Default The default value is 1500.

Mode Interface Config

4.2.2.11. *Encapsulation*

This command configures the link layer encapsulation type for the packet.

Format encapsulation {ethernet | snap}

Fields	Definition
ethernet	The link layer encapsulation type is ethernet.
snap	The link layer encapsulation type is SNAP.

Default The default value is ethernet.

Mode Interface Config

Restrictions Routed frames are always Ethernet encapsulated when a frame is routed to a VLAN.

4.3. VLAN Routing Commands

4.3.1. Configuration commands

4.3.1.1. *Interface vlan*

This command creates a VLAN routing interface.

To delete a VLAN routing interface, use the **no** form of this command.

Format interface vlan <vlan-id>

no interface vlan <vlan-id>

Fields	Definition
<vlan-id>	The VLAN ID used for this interface. The range of VLAN ID is from 1 to 4093.

Default None

Mode Global Config

5. IP Multicast Commands

5.1. Internet Group Management Protocol (IGMP) Commands

This section provides a detailed explanation of the IGMP commands. The commands are divided into the following different groups:

Show commands are used to display device settings, statistics and other information.

Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

5.1.1. Show commands

5.1.1.1. *Show ip igmp*

This command displays the system-wide IGMP information.

Format show ip igmp

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value.
IGMP Router-Alert check	This field displays the administrative status of Router-Alert validation for IGMP packets.
Interface	Valid slot and port number separated by forward slashes.
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
Operational-Status	This field indicates the current state of IGMP on this interface. Possible values are Operational or Non-Operational.

5.1.1.2. *Show ip igmp groups*

This command displays the registered multicast groups on the interface. If “detail” is specified this command displays the registered multicast groups on the interface in detail.

Format show ip igmp groups {<slot/port> | vlan <vlan-id>} [detail]

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.
[detail]	Display details of subscribed multicast groups.

Default None

Mode Privileged EXEC

Display Message

Fields	Definition
IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays the subnet mask of the interface participating in the multicast group.
Interface Mode	This displays whether IGMP is enabled or disabled on this interface. *// The following fields are not displayed if the interface is not enabled:*
Querier Status	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Groups	This displays the list of multicast groups that are registered on this interface. *If detail is specified, the following fields are displayed:*
Multicast IP Address	This displays the IP Address of the registered multicast group on this interface.

Last Reporter	This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.
Up Time	This displays the time elapsed since the entry was created for the specified multicast group address on this interface.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out.
Version1 Host Timer	This displays the time remaining until the local router assumes that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.
Version2 Host Timer	This displays the time remaining until the local router assumes that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface.This could be an integer value or "-----" if there is no Version 2 host present.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

5.1.1.3. *Show ip igmp interface*

This command displays the IGMP information for the interface.

Format show ip igmp interface {<slot/port> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.

IP Address	This displays the IP address of the interface participating in the multicast group.
Subnet Mask	This displays the subnet mask of the interface participating in the multicast group.
IGMP Admin Mode	This field displays the administrative status of IGMP. This is a configured value
Interface Mode	This field indicates whether IGMP is enabled or disabled on the interface. This is a configured value.
IGMP Version	This field indicates the version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.
Query Interval (secs)	This field indicates the frequency at which IGMP Host-Query packets are transmitted on this interface. This is a configured value.
Query Max Response Time (1/10 of a second)	This field indicates the maximum query response time advertised in IGMPv2 queries on this interface. This is a configured value.
Robustness	This field displays the tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface. This is a configured value.
Startup Query Interval (secs)	This value indicates the interval between General Queries sent by a Querier on startup. This is a configured value.
Startup Query Count	This value is the number of Queries sent out on startup, separated by the Startup Query Interval. This is a configured value.
Last Member Query Interval (1/10 of a second)	This value indicates the Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This is a configured value
Last Member Query Count	This value is the number of Group-Specific Queries sent before the router assumes that there are no local members. This is a configured value.

5.1.1.4. *Show ip igmp interface membership*

This command displays the list of interfaces that have registered in the multicast group.

Format show ip igmp interface membership <multiipaddr> [detail]

Fields	Definition
< multiipaddr >	A multicast IP address.
[detail]	Display details of subscribed multicast groups.

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
Interface IP	This displays the IP address of the interface participating in the multicast group.
State	This displays whether the interface has IGMP in Querier mode or Non-Querier mode.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

If detail is specified, the following fields are displayed:

Fields	Definition
Interface	Valid slot and port number separated by forward slashes.
Group Compatibility Mode	The group compatibility mode (v1, v2 or v3) for the specified group on this interface.
Source Filter Mode	The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.
Source Hosts	This displays the list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified

	multicast group IP Address. This is “-----” for IGMPv1 and IGMPv2 Membership Reports.
Expiry Time	This displays the amount of time remaining to remove this entry before it is aged out. This is “- ----” for IGMPv1 and IGMPv2 Membership Reports.

5.1.1.5. *Show ip igmp interface stats*

This command displays the IGMP statistical information for the given interface. The statistics are only displayed when the interface is enabled for IGMP.

Format show ip igmp interface stats {<slot/port> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is from 1 to 4093.

Default None

Mode Privileged EXEC
User EXEC

Display Message

Fields	Definition
Querier Status	This field indicates the status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.
Querier IP Address	This field displays the IP Address of the IGMP Querier on the IP subnet to which this interface is attached.
Querier Up Time	This field indicates the time since the interface Querier was last changed.
Querier Expiry Time	This field displays the amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.
Wrong Version Queries	This field indicates the number of queries received whose IGMP version does not match the IGMP version of the interface.
Number of Joins	This field displays the number of times a group membership has been added on this interface.

Number of Groups	This field indicates the current number of membership entries for this interface.

5.1.2. Configuration commands

5.1.2.1. *Ip igmp*

This command sets the administrative mode of IGMP in the router to active.

To set the administrative mode of IGMP in the router to inactive, use the no form of this command.

Format ip igmp

no ip igmp

Default Disable

Mode Global Config

Interface Config

5.1.2.2. *Ip igmp last-member-query-count*

This command sets the number of Group-Specific Queries sent by the interface before the router assumes that there are no local members on the interface.

To reset the number of Group-Specific Queries to the default value, use the no form of this command.

Format ip igmp last-member-query-count <1-20>

no ip igmp last-member-query-count

Fields	Definition
<1-20>	The range for last-member-query-count is from 1 to 20.

Default **2**

Mode Interface Config

5.1.2.3. *Ip igmp last-member-query-interval*

This command configures the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface.

To reset the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value, use the no form of this command.

Format ip igmp last-member-query-interval <0-255>

no ip igmp last-member-query-interval

Fields	Definition
<0-255>	The range for last-member-query-interval is from 0 to 255 tenths of a second.

Default 10 tenths of a second

Mode Interface Config

5.1.2.4. *Ip igmp query-interval*

This command configures the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

To reset the query interval for the specified interface to the default value, use the no form of this command.

Format ip igmp query-interval <1-31744>

no ip igmp query-interval

Fields	Definition
<1-31744>	The range for query-interval is from 1 to 31744 seconds.
IGMP version 3	range 1-31744, version 2: range 1-3600, version 1: range 1-3600

Default 125 seconds

Mode Interface Config

5.1.2.5. *Ip igmp query-max-response-time*

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface. The time interval is specified in tenths of a second.

To reset the maximum response time interval for the specified interface to the default value, use the no form of this command.

Format ip igmp query-max-response-time <0-31744>

no ip igmp query-max-response-time

Fields	Definition
<1-31744>	The range for query-max-response-time is from 0 to 31744 tenths of a second.
IGMP version 3	range 0-31744, version 2: range 0-255, version 1: range 0-255

Default 100

Mode Interface Config

5.1.2.6. *Ip igmp robustness*

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface.

To reset the robustness value to the default value, use the no form of this command.

Format ip igmp robustness <1-255>

no ip igmp robustness

Fields	Definition
<1-255>	The range for robustness is from 1 to 255.

Default 2

Mode Interface Config

5.1.2.7. *Ip igmp startup-query-count*

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface.

To reset the number of Queries sent out on startup to the default value, use the no form of this command.

Format ip igmp startup-query-count <1-20>

no ip igmp startup-query-count

Fields	Definition
<1-20>	The range for startup-query-count is from 1 to 20.

Default 2

Mode Interface Config

5.1.2.8. *Ip igmp startup-query-interval*

This command sets the interval between General Queries sent by a Querier on startup on the interface. The time interval value is in seconds.

To reset the interval between General Queries sent by a Querier on startup on the interface to the default value, use the no form of this command.

Format ip igmp startup-query-interval <1-300>

no ip igmp startup-query-interval

Fields	Definition
<1-300>	The range for startup-query-interval is from 1 to 300 seconds.

Default 31

Mode Interface Config

5.2. IPv4 Protocol Independent Multicast (PIM) Commands

5.2.1. Show commands

5.2.1.1. *Show ip pim*

This command displays the system-wide information for PIM-SM.

Format show ip pim

Default **None**

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
PIM Mode	Indicates the PIM mode is sparse (PIM-SM)
Data Threshold Rate (Kbps)	Rate (in kbps) of SPT Threshold
Interface	slot/port, or VLAN ID
Interface Mode	Indicates whether PIM is enabled or disabled on this interface
Operational Status	The current state of PIM on this interface: Operational or Non-Operational.

5.2.1.2. *Show ip pim bsr-router*

This command displays the bootstrap router (BSR) information.

Format show ip pim bsr-router {candidate | elected}

Default **None**

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
BSR Address	IP address of the BSR
BSR Priority	Priority as configured in the „ip pim bsr-candidate“ command
BSR Hash Mask Length	Length of a mask (maximum 32 bits) that is to be ANDed with the group address before the hash function is called. This value is configured in the ip pim bsrcandidate command
C-BSR Advertisement Interval(secs)	Indicates the configured C-BSR Advertisement interval with which the router, acting as a C-BSR, will periodically send the C-BSR advertisement messages.
Next Bootstrap Message(hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR

5.2.1.3. *Show ip pim interface*

This command displays the interface information for PIM on the specified interface. If no interface is specified, the command displays the status parameters for all PIM-enabled interfaces.

Format show ip pim interface [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default **None**

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Interface	slot/port
Mode	Indicates the PIM mode enabled on the interface is sparse

Hello Interval	The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds
Join Prune Interval	The join/prune interval for the PIM router. The interval is in seconds
DR Priority	The priority of the Designated Router configured on the interface.
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface
Neighbor Count	The number of PIM neighbors learned on this interface. This is a dynamic value and is shown only when a PIM interface is operational
Designated Router	The IP address of the elected Designated Router for this interface. This is a dynamic value and will only be shown when a PIM interface is operational.

5.2.1.4. *Show ip pim neighbor*

This command displays PIM neighbors discovered by PIMv2 Hello messages. If the interface number is not specified, this command displays the neighbors discovered on all the PIM enabled interfaces.

Format show ip pim neighbor [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port>	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default **None**

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Neighbor Address	The IP address of the neighbor on an interface
Interface	slot/port

Up Time	The time since this neighbor has become active on this interface
Expiry Time	The expiry time of the neighbor on this interface
DR Priority	The DR Priority configured on this Interface (PIM-SM only)
BSR Border	Identifies whether this interface is configured as a bootstrap router border interface

i DR Priority is applicable only when sparse-mode configured routers are neighbors. Otherwise, NA is displayed in this field

5.2.1.5. *Show ip pim rp mapping*

Use this command to display all active group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). Use the optional parameters to limit the display to a specific RP address or to view group-to-candidate RP or group to Static RP mapping information.

Format show ip pim rp mapping [{<rp-address> | candidate | static}]

Default **None**

Mode Privileged Exec

User Exec

Display Message

Fields	Definition
RP Address	The IP address of the RP for the group specified
Group Address	The IP address and prefix length of the multicast group
Group Mask	The subnet mask associated with the group
Origin	Indicates the mechanism (BSR or static) by which the RP was selected
Expiry Time	The expiry time of the RP mapping

C-RP Advertisement Interval(secs)	Indicates the configured C-RP Advertisement interval with which the router, acting as a C-RP, will periodically send the C-RP advertisement messages.
Next Candidate RP Advertisement (hh:mm:ss)	Time (in hours, minutes, and seconds) in which the next C-RP Advertisement is due from this Router

5.2.1.6. *Show ip pim rp-hash*

This command displays which rendezvous point (RP) is being used for a specified group.

Format show ip pim rp-hash <group-address>

Fields	Definition
<group-address>	the multicast group address for the start of the range of addresses to be excluded. The address must be in the range of 239.0.0.0 through 239.255.255.255.

Default **None**

Mode Privileged Exec

User Exec

Display Message

Fields	Definition
RP Address	The IP address of the RP for the group specified
Type	Indicates the mechanism (BSR or static) by which the RP was selected

5.2.1.7. *Show ip pim ssm*

This command displays the configured source specific IP multicast addresses. If no SSM Group range is configured, this command output is No SSM address range is configured.

Format show ip pim ssm

Default **None**

Mode Privileged Exec

User Exec

Display Message

Fields	Definition
Group Address	The IP multicast address of the SSM group
Prefix Length	The network prefix length

5.2.1.8. *Show ip pim statistics*

This command displays statistics for the received PIM control packets per interface. This command displays statistics only if PIM sparse mode is enabled.

Format show ip pim statistics [{<slot/port> | vlan <vlan-id>}]

Fields	Definition
<slot/port >	Interface number.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.

Default **None**

Mode Privileged Exec
User Exec

Display Message

Fields	Definition
Intf	The PIM-enabled routing interface.
Stat	Rx: Packets received, Tx: Packets transmitted.
Hello	The number of PIM Hello messages.
Register	The number of PIM Register messages.
Reg-Stop	The number of PIM Register-stop messages.
BSR	The number of PIM Boot Strap messages.

Assert	The number of PIM Assert messages.
CRP	The number of PIM Candidate RP Advertisement messages.

5.2.2. Configuration commands

5.2.2.1. *Ip pim bsr-candidate*

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

To remove a configured candidate bootstrap router (C-BSR), use the no form of this command.

Format ip pim bsr-candidate interface {<slot/port> | vlan <vlan-id>} <hash-mask-length> [<priority>] [interval <1-16383>]

no ip pim bsr-candidate interface {<slot/port> | vlan <vlan-id>}

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<hash-mask-length>	BSR hash-mask length. The range of the mask is 0 to 32.
<priority>	BSR priority. The range of the priority is 0 to 255.
<interval>	BSR candidate advertisement interval. The range of the priority is 1 to 16383.

Default **Disable**

Mode Global Config

Display Message

Fields	Definition
hash-mask-length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. All groups with the same seed hash correspond to the same RP. For example, if this value was 24, only the first 24 bits of the group addresses matter. This allows you to get one RP for multiple groups.
Priority	Priority of the candidate BSR. The range is an integer from 0 to 255. The BSR with the larger priority is preferred. If the priority

	values are the same, the router with the larger IP address is the BSR. The default value is 0.

This command takes effect only when PIM-SM is configured as the PIM mode

5.2.2.2. *Ip pim rp-address*

This command is used to statically configure the RP address for one or more multicast groups. The parameter rp-address is the IP address of the RP. The parameter groupaddress is the group address supported by the RP. The parameter groupmask is the group mask for the group address. The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

To remove a configured RP address for one or more multicast groups, use the no form of this command.

Format ip pim rp-address <rp-address> <group-address> <group-mask> [override]

no ip pim rp-address <rp-address> <group-address> <group-mask>

Fields	Definition
<rp-address>	Specifies the rp address.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group mask.
[overide]	Indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

Default **0**

Mode Global Config

This command takes effect only when PIM-SM is configured as the PIM mode

5.2.2.3. *Ip pim rp-candidate*

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

To disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR), use the no form of this command.

Format ip pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address> <group-mask> [interval <1-16383>]

no ip pim rp-candidate interface {<slot/port> | vlan <vlan-id>} <group-address> <group-mask>

Fields	Definition
<slot/port>	Valid slot and port number separated by forward slashes.
<vlan-id>	VLAN ID. The range of VLAN ID is 1 to 4093.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group mask.
[interval]	Indicates the RP candidate advertisement interval. The range is from 1 to 16383. The default value is 60 seconds.

Default **None**

Mode Global Config

i This command takes effect only when PIM-SM is configured as the PIM mode

5.2.2.4. *Ip pim sparse*

This command enables the administrative mode of PIM-SM in the router.

To set the administrative mode of IPv4 PIM-SM in the router to inactive, use the no form of this command.

Format ip pim sparse

no ip pim sparse

Default **Disable**

Mode Global Config

5.2.2.5. *Ip pim ssm*

Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses.

To disable the specified Source Specific Multicast (SSM) range, use the no form of this command.

Format ip pim ssm {default | <group-address> <group-mask>}

no ip pim ssm {default | <group-address> <group-mask>}

Fields	Definition
Default	Defines the SSM range access list 232/8.
<group-address>	Specifies the group address.
<group-mask>	Specifies the group-mask.

Default **Disable**

Mode Global Config

5.2.2.6. *Ip pim*

This command administratively enables PIM on an interface or range of interfaces.

To set the administrative mode of PIM on an interface to disabled, use the no form of this command.

Format ip pim

no ip pim

Default **Disable**

Mode Interface Config

5.2.2.7. *Ip pim bsr-border*

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface or range of interfaces.

To disable the interface from being the BSR border, use the no form of this command.

Format ip pim bsr-border

no ip pim bsr-border

Default **Disable**

Mode Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode

5.2.2.8. *Ip pim dr-priority*

Use this command to set the priority value for which a router is elected as the designated router (DR). This command can be configured on a single interface or a range of interfaces.

To reset the priority value to the default value for which a router is elected as the designated router (DR), use the no form of this command.

Format ip pim dr-priority <0-4294967294>

no ip pim dr-priority

Fields	Definition
<0-4294967294>	The range for dr-priority is from 0 to 4294967294.

Default **1**

Mode Interface Config

This command takes effect only when PIM-SM is configured as the PIM mode

5.2.2.9. *Ip pim hello-interval*

Use this command to configure the PIM hello interval for the specified router interface or range of interfaces.

To reset the PIM hello interval to the default value, use the no form of this command.

Format ip pim hello-interval <0–18000>

no ip pim hello-interval

Fields	Definition

<0-18000>	The range for hello-interval is from 0 to 18000 seconds.

Default **30**

Mode Interface Config

5.2.2.10. *Ip pim join-prune-interval*

This command is used to configure the join/prune interval for the PIM-SM router on an interface or range of interfaces. The join/prune interval is specified in seconds.

To reset the PIM join/prune interval to the default value, use the no form of this command.

Format ip pim join-prune-interval <0-18000>

no ip pim join-prune-interval

Fields	Definition
<0-18000>	The range for hello-interval is from 0 to 18000 seconds.

Default **60**

Mode Interface Config

i This command takes effect only when PIM-SM is configured as the PIM mode.